Tomi Ruha

Cybersecurity of Computer Networks

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Thesis

14 April 2018

Metropolia

Author(s) Title Number of Pages Date	Tomi Ruha CyberSecurity of Computer Networks 49 pages 14 April 2018
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Communication Networks and Applications
Instructor(s)	Erik Pätynen, Senior Lecturer

The subject of this thesis is the basics of cybersecurity and particularly from companies' points of view. The thesis introduces policies, processes, controls and some technology for protecting a network and most important in cybersecurity is security and awareness training for people. Furthermore, information security and cybersecurity is a never-ending process rather than a project. However, improving security areas in a company can start as a project but the continuum has to be a process.

First some examples of confidentiality, availably and integrity which are three pillars in information security and in cybersecurity are discussed. This thesis is more from a defensive cybersecurity point of view rather than an offensive cybersecurity point of view, but both trends are equally important. Finally, network threats and mitigation of common threats are studied.

Important processes like Disaster Recovery Planning (DRP) are discussed, which is ignored in many companies. It is part of the Business Continuity Plan (BCP). Change management is a good process especially when handling medium to critical applications and servers. Center of Internet Security (CIS) top five controls, which every company should have implemented for better overall security are discussed. The larger the company, the more controls should be applied from the top 20 list of controls.

This document helps to understand the meaning of the cybersecurity in a computer world where individuals' lives might be dependent on well-built defenses on the networks. All-over the world peoples personal data might be stored on the storage and can be taken like a low hanging fruit from a tree if security defenses are neglected by a company leadership.

Keywords	cybersecurity, information security, network security, CIA, AIC, GDPR, security policy, security control

Tekijä Otsikko Sivumäärä Aika	Tomi Ruha Tietoverkkojen kyberturvallisuus 49 sivua 14.4.2018
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikka
Ammatillinen pääaine	Communication Networks and Applications
Ohjaaja	Lehtori Erik Pätynen

Insinöörityön tarkoituksena oli koota yhteen kyberturvallisuuden perusteet yrityksen näkökulmasta katsottuna. Työssä perehdyttiin tietoturvakäytänteisiin, -prosesseihin ja -kontrolleihin, muutamiin teknologioihin, joilla suojata verkkoa, sekä yhtenä tärkeimpänä tietoturva- ja tietoisuuskoulutuksiin. Tietoturva ja kyberturva eivät ole projekti vaan jatkuva prosessi yrityksissä. Kyberturvaa parantavat toimenpiteet voidaan aloittaa projektina, mutta projektin päättymisen jälkeen toimenpiteiden on jatkuttava prosessina.

Luottamuksellisuus, saatavuus ja eheys (CIA, Confidentiality, Integrity, Availability) ovat tietoturvan kolme tukipilaria. Insinöörityössä perehdyttiin kyberturvallisuuteen puolustavan kyberturvallisuuden näkökulmasta, mutta tarkasteltiin myös hyökkäävää kyberturvallisuutta. Nämä kaksi kulkevat käsi kädessä ja ovat yhtä tärkeitä osa-alueita kyberturvallisuudessa.

Työssä nostettiin esiin muutamia tärkeitä prosesseja, joiden pitäisi olla käytössä joka yrityksessä yrityksen koosta riippumatta. Niihin kuuluvat katastrofien elvytyssuunnitelmat, jotka ovat unohtuneet monelta yritykseltä toteuttaa. Ne ovat osa liiketoiminnan jatkuvuussuunnitelmaa. Muutoksenhallintaprosessin on hyvä olla olemassa etenkin niissä yrityksissä, joissa ylläpidetään tai tarjotaan palveluna asiakkaalle kriittisiä palveluita. Jokaisessa yrityksessä pitäisi olla käytössä ainakin nämä viisi tärkeintä turvallisuustoimenpidettä, jotka nostavat kyberturvallisuuden tasoa: valtuutettujen ja luvattomien laitteiden luettelo, valtuutettujen ja luvattomien ohjelmistojen luettelo, laitteistojen ja ohjelmistojen turvalliset konfiguroinnit, jatkuva haavoittuvuusarviointi ja kunnostaminen sekä hallittu hallintatunnuksien käyttäminen.

Insinöörityö auttaa ymmärtämään kyberturvallisuuden merkityksen nykyisessä tietotekniikan valloittamassa maailmassa, jossa yksilöiden elämä saattaa olla kiinni siitä, miten yrityksen tietoturva on toteutettu. Ihmisten henkilökohtaisen tiedon suojaamatta jättäminen koituu kohtalokkaaksi tulevaisuudessa, ja näiden asioiden käyttöön tuomisen on lähdettävä yrityksen johdosta käsin.

Avainsanat	kyberturvallisuus, tietoturva, tietoverkkojen tietoturva, CIA, AIC, GDPR, tietoturvakäytännöt, tietoturvakontrollit

Metropolia

Contents

1 Introduction 1

1.1 Objectives 1
1.2 Scope and Structure of the Thesis 2
1.3 Abbreviations 2

2 CIA Model 3

2.1 Confidentiality 4
2.2 Integrity 5
2.3 Availability 9

3 Mandatory Processes for Companies 12

3.1 Disaster Recovery Planning 12
3.2 Change Management 13

4 Security Controls 15

4.1 Inventory of Authorized and Unauthorized Devices 16
4.2 Inventory of Authorized and Unauthorized Software 17
4.3 Secure Configurations for Hardware and Software 17
4.4 Continuous Vulnerability Assessment and Remediation 18
4.5 Controlled Use of Administrative Privileges 18

5 Overview of General Data Protection Regulation 19

5.1 Personal Data 19
5.2 Data Protection Deviations 20
5.3 GDPR and Individual Rights 20

6 Physical Security 20

6.1 Uninterruptible Power Supply 20
6.2 Datacenter Cooling Systems, Temperature and Humidity 21
6.3 Location of the Equipment 22

7 Defense of the Network 23

7.1 Endpoint Protection 24
7.2 Firewalls 24

7.3 Intrusion Detection Systems 27
7.4 Network Monitoring 29
7.5 Virtual Private Network 29
7.6 Wireless Security 30
7.7 Centralized User Account Management 31
7.8 Data Loss Prevention 33
7.9 Documentation 33
7.10 Employee Training 34
7.11 Security Audit and Security Scanning 34
7.12 SIM, SEM, SIEM 35

8 Network Threats 37

8.1 Proactive Reaction to Threats 38
8.2 Critical infrastructures 38
8.3 Data Breaches 41
8.4 Reconnaissance 41
8.5 Advanced Persistent Threats 42
8.6 Denial of Service 43
8.7 Ransomware 44

9 Mitigation of Many Threats 44

9.1 Patch Operating Systems and Utilities 45
9.2 Patch Hardwares Firmware 45
9.3 Unknown Peripherals 46
9.4 Two-factor Authentication 46
9.5 Change Default Configurations of Devices 46
9.6 Endpoint Protection Software Installed 47
9.7 E-mails, Attachments and Links 47

10 Conclusions 47

References 50

List of abbreviations

AAA	Authentication, authorization, accounting
AD	Active directory
ADDS	Active directory domain services
AES	Advanced encryption standard
AI	Artificial intelligence
AIC	Availability, integrity, confidentiality
AP	Access point
APT	Advanced persistent threats
AWS	Amazon web services
BCP	Business continuity planning
BYOD	Bring your own device
CAB	Change advisory board
CIA	Central Intelligence Agency
CIA	Confidentiality, integrity, availability
CIS	Canter of internet security
CPU	Central processing unit
CVSS	Common vulnerability scoring system
DDOS	Distributed denial of service

DLP	Data loss prevention
DNS	Domain name system
DOS	Denial of service
DR	Disaster recovery
DRP	Disaster recovery planning
EAP	Extensible authentication protocol
EP	Endpoint protection
EU	European Union
GDPR	General data protection regulation
HIDS	Host-based intrusion detection system
HMAC	Hash-based message authentication code
HTTP	Hyper text transfer protocol
HTTPS	Hyper text transfer protocol over ssl
I/O	Input/output
ICT	Information and communication technology
IDS	Intrusion detection system
IETF	Internet engineering task force
IoT	Internet of things
IP	Internet protocol

IPS	Intrusion prevention system
IPsec	Internet protocol security
ISP	Internet service provider
IT	Information technology
ITIL	Information technology infrastructure library
LAN	Local area network
LDAP	Lightweight directory access protocol
MBTF	Mean time between failures
MD5	Message-digest 5
MTTF	Mean time to failure
MTTR	Mean time to repair
NGFW	Next generation firewall
NHS	National health service
NIC	Network interface controller
NIS	Network information system
NSA	National security agency
OS	Operating system
OSI	Open systems interconnection
RAM	Random access memory

RFC	Request for change
RFC	Request for comments
RPO	Recovery point objective
RTO	Recovery time objective
SaaS	Software as a service
SCADA	Supervisory control and data acquisition
SCAP	Security content automation protocol
SCCM	System center configuration manager
SCOM	System center operations manager
SEM	Security event management
SHA	Secure hash algorithm
SIEM	Security information event management
SIM	Security information management
SLA	Service level agreement)
SPI	Stateful packet inspection
SSH	Secure shell
SSID	Service set identifier
SSL	Secure sockets layer
SWAT	Securing web applications technologies

TDOS	Telephony denial of service
TLS	Transport layer security
UPS	Uninterruptible power supply
USB	Universal serial bus
VLAN	Virtual local area network
VM	Virtual machine
VPN	Virtual private network
WAF	Web application firewall
WAN	Wide area network
WEP	Web equivalent privacy
WLAN	Wireless local area network
WMI	Windows management instrumentation
WPA	Wi-Fi protected access
WPA2	Wi-Fi protected access 2
XSS	Cross-site scripting

1 Introduction

1.1 Objectives

The aim of the thesis is to discuss the cybersecurity world from companies point of view. The cybersecurity is a very interesting subject and this subject is quite current all over the world.

The cybersecurity is not a project, however, it is a never-ending process. The cybersecurity and information security implementation can start as a project, but the continuum will be a process. Security must be always in mind and one must never take shortcuts in security issues or in security planning. Attackers like shortcuts taken in security planning and implementation. This thesis is about how to defend a company's network and assets within a network and to protect humans as well increase their security awareness by yearly training sessions. Defensive and offensive cybersecurity walk together. They are both equally important. Most companies focus on defensive side and if something needs to be tested, mostly that will be bought from a cybersecurity company.

In the past companies had their own datacenters and defense was like a fortress. However today defenses must be more resilient and dynamic because employees use remote connections to the network and many services might run outside of company network. Communicating remotely with internal servers with encrypted connections is a mandatory feature today. Companies use cloud services more and more today and there will be more and more hybrid datacenters with cloud services like Azure, Amazon Web Services (AWS), google and others. Cloud services with their own datacenters work together because companies can get somewhat easily more resources from cloud services when scaling of infrastructure is required. Services are going more to hybrid systems, so cybersecurity needs to be designed from a different point of view. Network resilience is more important now, and it needs to be expected that firewalls can be breached but attackers do not have a chance to get any foothold from the network.

Another goal of this thesis is to build a general perception of network cybersecurity and what should be taken into a company cybersecurity plan to increase the overall security

baseline. The document is not technical and does not include configurations of any devices or software. The objective of the work is to introduce cybersecurity within companies and to give recommendations, and thoughts about what can be done better or what is missing in companies' security policies. The cybersecurity or information security cannot be ignored, so hopefully this document will give a start for better overall cybersecurity awareness.

1.2 Scope and Structure of the Thesis

The CIA model is introduced in chapter 2 which is very important and some good policies and controls in chapters 3 and 4 which should be implemented. Quick look up to GDPR is in chapter 5 which is a current topic and important to everybody. Endpoint protection, firewalls, intrusion detection systems, and security information and event management systems are introduced in chapter 5 but configurations of any kind of systems are beyond the scope of this document. This document is about defensive cybersecurity and is not a deep dive into cybersecurity. Physical security is important and that is introduced in chapter 6. Network defense is introduced in chapter 7 but offensive cybersecurity is beyond of the scope. This document briefly discusses the offensive side in chapters 8 and 9. Chapter 8 is about network threats. There are more threats all the time, but everything cannot be covered. Chapter 9 is about how to mitigate common threats in a company's network.

Unfortunately securing web applications is not included in this document even though it is a very important subject. SANS Securing Web Applications Technologies (SWAT) is a good to meet this subject. Risk management in software development is not included on the document even though that topic is important as well, but information can be found on the internet. (https://software-security.sans.org, 2018 and http://www.castsoftware.com, 2018)

1.3 Abbreviations

Abbreviations with multiple meanings are used in this thesis, such as RFC (Request for Comment) and CIA (Confidentiality, Integrity, Availability). Their meanings in this document are explained to avoid confusion.

Request for Comment (RFC) is Internet Engineering Task Force (IETF) standard abbreviation and should not be confused with Information Technology Infrastructure Library (ITIL) abbreviation Called Request for change (RFC). It is presented in section 3.2 in this document. (https://www.ietf.org, 2018 and https://wiki.en.it-processmaps.com, 2018)

Confidentiality, Integrity, Availability (CIA) is the term used in this document in chapter 2: CIA Model (Triad) and is a common term in information security and in cybersecurity. Do not confuse Central Intelligence Agency (CIA) with the CIA model.

2 CIA Model

The CIA (Confidentiality, Integrity, Availability) is a part of traditional security and cybersecurity. The CIA model is about to guide policies for cybersecurity in companies and the CIA is illustrated in Figure 1. The CIA model is also referred as AIC (Availability, Integrity, Confidentiality) to avoid confusion with other one called CIA (Central Intelligence Agency) but furthermore the CIA elements are the three most crucial components related to security. In the following sections, CIA model is explained more specifically with examples each part of the model. (http://whatis.techtarget.com, 2017)

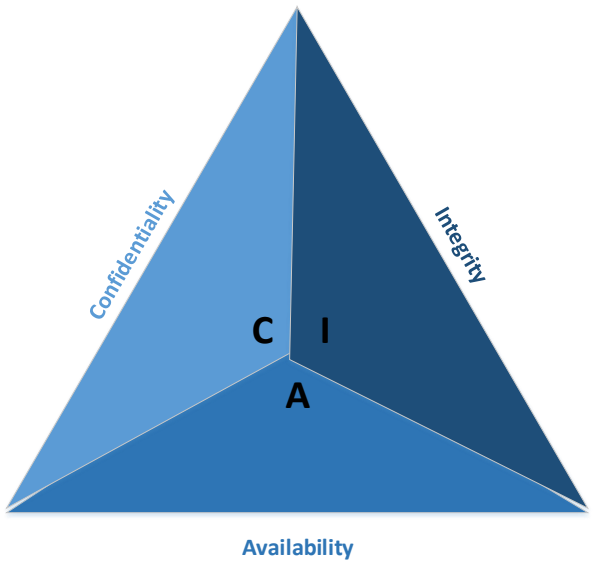

Figure 1. CIA Triad (http://whatis.techtarget.com,2017)

2.1 Confidentiality

Confidentiality is privacy and authorization. When sensitive data is disclosed to unauthorized people that is loss of confidentiality. As an example, if an unauthorized user can see payroll data of the other employees, it is loss of confidentiality. In that case privacy and authorization has failed. Protecting against loss of confidentiality is access controls and encryption of data and databases. Modern encryption algorithms are quite secure like Advanced Encryption Standard (AES) with key length of 256 bits. With AES can be used shorter key lengths like 128 bits and 192 bits but 256 bits is recommended. The longer the key is the harder it is to breach the encryption which means it is harder to access data itself without decryption keys. When the user is authenticated, and authorization is completed the user has access to system or user is denied access to a system based on their access rights. Figure 2 illustrates loss of confidentiality. (http://www.pearsonitcertification.com, 2017 and https://www.globalsign.com, 2018)

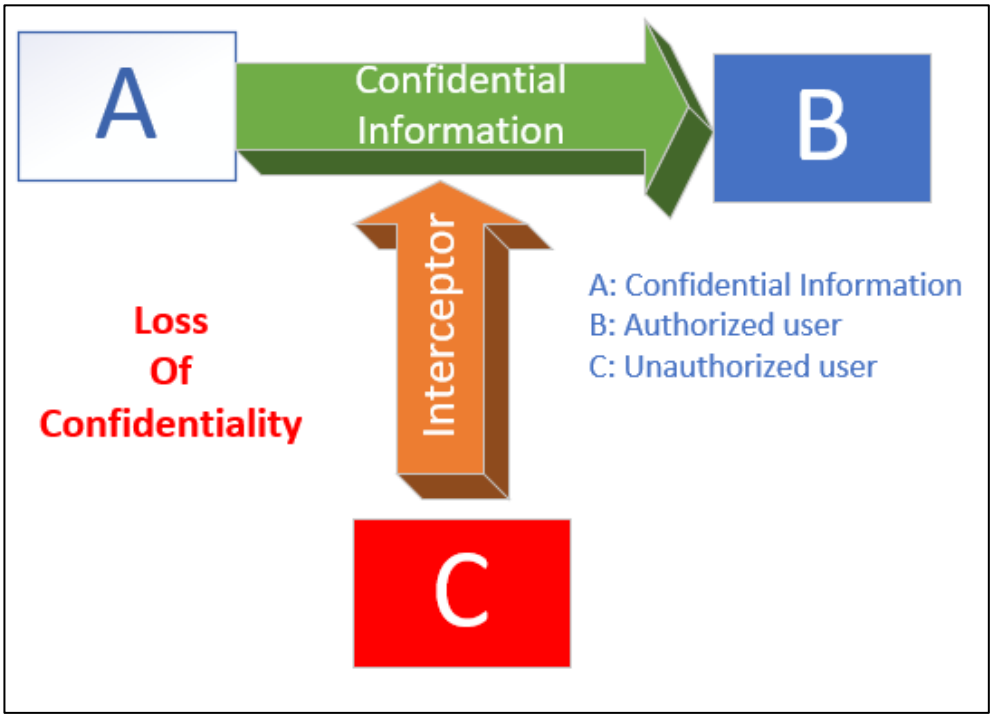

Figure 2. Loss of confidentiality

Confidentiality in data communication is vital. Virtual Private Network (VPN) is an appropriate solution for securing communication between users and a target network or network-to-network (Site-To-Site) communication over the internet which increases confidentiality. But the VPN solutions cannot be used everywhere, therefore web surfing, paying bills and all kind of sensitive data should be handled by use of encrypted traffic. The Transport Layer Security (TLS) is replacing SSL versions 2.0 and SSL 3.0, which are deprecated by Internet Engineering Task Force (IETF) due to vulnerabilities like the POODLE and the DROWN in SSL protocol versions. Hyper Text Transfer Protocol over SSL (HTTPS), which makes using of internet resources more secure increasing confidentiality and privacy as well which very important. There are many websites which do not use HTTPS. If a website does not use encrypted traffic users should be more careful especially if confidential data is handled in that service and no one should never give any confidential information on unencrypted sites. If a site is encrypted sensitive data should not be given if that is not necessary. Do not give confidential information just because a site requests the data. (https://www.wired.com, 2018 and https://www.globalsign.com, 2018)

2.2 Integrity

The integrity is trust and accuracy. Loss of integrity means that data has been modified or destroyed by an unauthorized individual or system configuration has been changed somehow forcing users to suffer from false information. Figure 3 is an illustrative example of loss of integrity when a user downloads a file from a server and hash has been changed from the original value, which means a file system has been tampered. (http://www.pearsonitcertification.com, 2017)

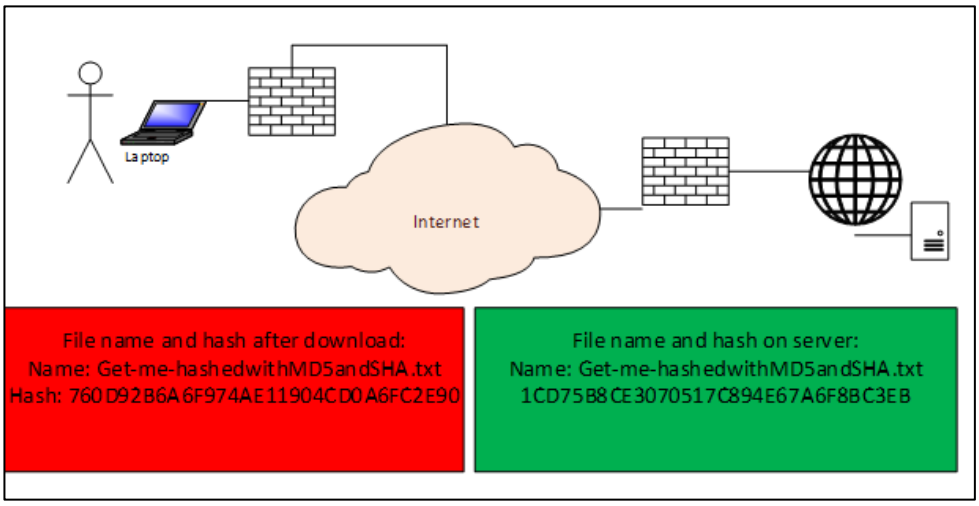

Figure 3. File integrity change

Protection against loss of integrity is hashing. In these examples a MD5 (Message Digest 5) and a SHA1 (Secure Hash Algorithm 1) hashing is used even though using these algorithms is not recommended anymore. Newer hashing algorithms like SHA2 and SHA3 should be used instead of MD5 or SHA1. The MD5 and the SHA1 hashing have a collision weakness that allows multiple input sources with same hashing result. It is obvious that with MD5 that happens more often than with SHA1. In a hashing example in Figure 4. There are MD5 and SHA1 calculations. Both calculations twice to see the hash will not change if the file content is not changed. (https://www.securityfocus.com, 2018 and https://www.computerworld.com, 2018)

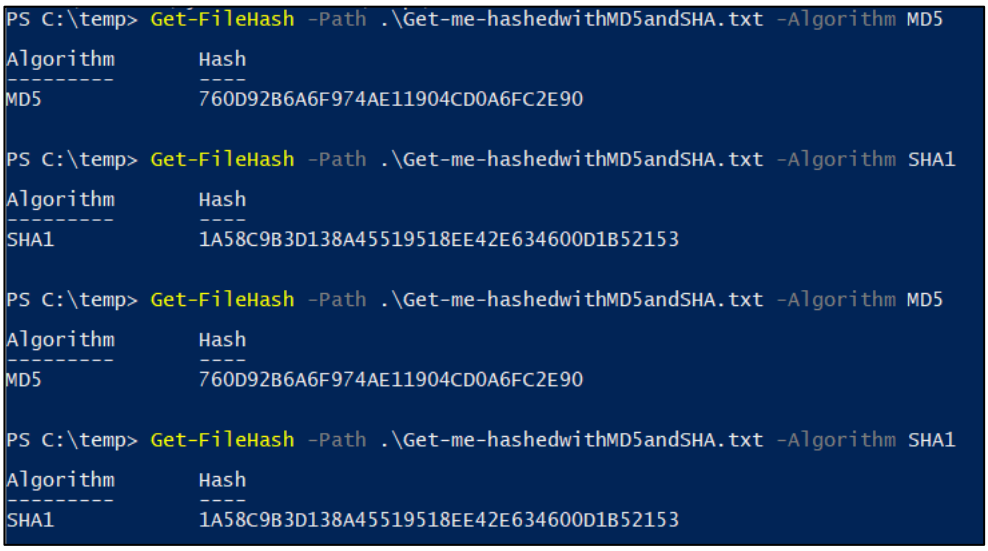

Figure 4. MD5 and SHA1 calculated

Renaming the file will not change the hash value which is good. See Figure 5 as an example of hash calculation after the file is renamed but the content remains the same.

Figure 5. MD5 and SHA1 calculated after renaming the file

Adding more content or editing a file content will change the hash drastically. See Figure 6 as an example of a recalculated hash. Changing the file content from hash me please to hash me please!! changes the hash drastically. If file hashes are taken periodically from important files. There is chance to see whether files are tampered in a file system. Any

kind of change inside the content will change the hash completely different. This is known as an avalanche effect and a hash allows to verify integrity of files. There is so much data in file servers which makes impossible to get daily hashes from every file stored in a system. Sometimes importance of files is hard to measure. Then files need to be marked as important and get file hashes often enough. (http://searchsecurity.tech-target.com, 2017)

```
PS C:\temp> type .\Get-me-hashedwithMD5andSHA-renamed.txt
hash me please
PS C:\temp>
PS C:\temp> type .\Get-me-hashedwithMD5andSHA-renamed.txt
hash me please!!
PS C:\temp> Get-FileHash -Path .\Get-me-hashedwithMD5andSHA-renamed.txt -Algorithm SHA1

Algorithm       Hash                                                                   P
---------       ----                                                                   -
SHA1            C67CB5B5CB666895D705F4D1CF96993D55F3BB3F                               C


PS C:\temp> Get-FileHash -Path .\Get-me-hashedwithMD5andSHA-renamed.txt -Algorithm md5

Algorithm       Hash                                                                   P
---------       ----                                                                   -
MD5             1CD75B8CE3070517C894E67A6F8BC3EB                                       C
```

Figure 6. MD5 and SHA1 calculated after changing file contents

As can be seen in Figure 7 both MD5 and SHA1 hashes are the same as in the original file tests illustrated in Figure 4. Hashing with stronger algorithms like SHA256 and SHA384 the hash calculation is longer. Chance of getting duplicate hashes on SHA256 or stronger algorithms are nearly impossible. The stronger the algorithm is, the more confidential the results are.

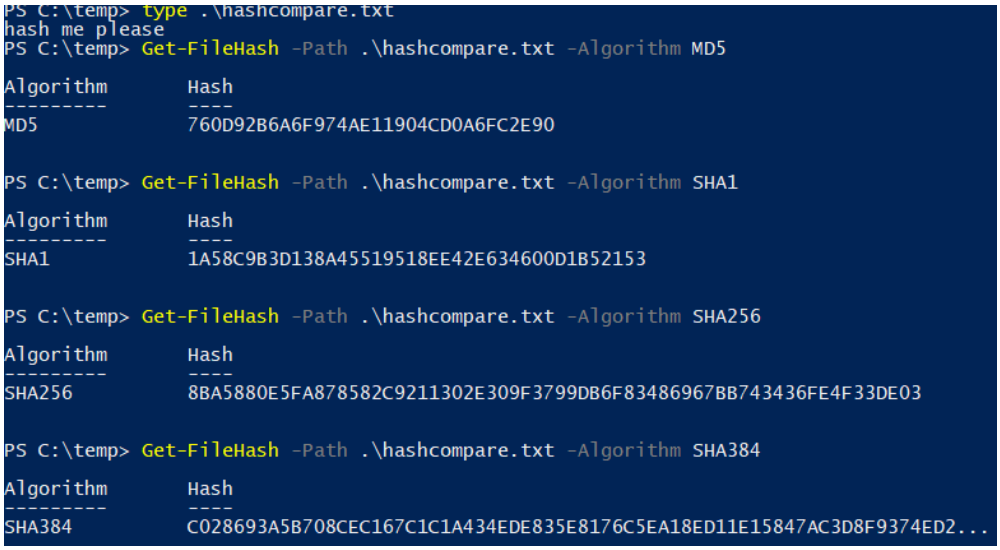

Figure 7. Comparing hashes

There is Hash-based Message Authentication Code (HMAC). A HMAC-MD5 or a HMAC-SHA1 first create a hash of message and then use a secret key to recalculate the hash making the hash stronger. This is alike as salting password hashes. The HMAC technique will increase integrity. (http://blogs.getcertifiedgetahead.com, 2018)

2.3 Availability

Loss of availability. A resource is not available whenever someone needs to access resource like a web store. Protection against the loss of availability is a fault tolerant system (redundant) with good backups of a systems and a fast restore process from backups. (http://www.pearsonitcertification.com, 2017)

It is obvious redundancy increases availability and increases SLA (Service Level Agreement). All devices have MTBF (Meantime Between Failures), which means how long specific device can operate without a failure. At least what is planned by a manufacturer. A MTTR (Mean Time To Repair) is the average time to get the device repaired after a failure. There is no tag for this in a device. Repair time more dependent on a SLA with a supplier of a device. There might be unexpected device failures, but they are quite rare in current devices. Mostly failing devices are revealed during the test phase. Every new device needs to be tested before installing them in production. In Figure 8 there are basic

formulas on how to count the MTBF, the MTTR and availability. (http://world-class-manufacturing.com, 2017)

$$\text{MTBF} = \frac{\text{(Total up time)}}{\text{(number of breakdowns)}}$$

$$\text{MTTR} = \frac{\text{(Total Down time)}}{\text{(number of breakdowns)}}$$

$$\text{Availability} = \frac{\text{MTBF}}{\text{MTBF + MTTR}}$$

Figure 8. Calculation formulas (Metropolia, Cybersecurity program, 2016)

In Table 1 there are illustrated values of possible availability. MTBF and MTTR calculations of one-month parallel connected devices. The reference device is Juniper Netscreen 50. All values are fictitious and cannot be guaranteed. In Figure 9 is the formula for a single device and In Figure 10 the formula itself for how to count availability of devices in parallel. Trendsetting values are used in calculations.

$$D_t = D_1$$

Figure 9. Formula for the single device (Metropolia, Cybersecurity program, 2016)

$$D_t = 1-(1-D_1) * (1-D_2) * (1-D_3)$$

Figure 10. Devices in a parallel formula (Metropolia, Cybersecurity program, 2016)

As table 1 illustrates parallel connectivity increases availability and three devices properly configured give near 100 % availability. In Table 1 is an example of devices in parallel. The first row in Table 1 and Table 2 illustrates a single device. A single device formula is illustrated in Figure 9. See in Table 1 the first row (single device) downtime

with 99.5 % availability would be approximately 4 hours in each month as an average downtime. (https://kb.juniper.net, 2017)

Table 1. Devices in a parallel

SLA	MTBF	MTTR	Failures	uptime	downtime	Devices (parallel)
99.5 %	726	4	1	726	4	1
99.997 %	726	4	1	726	4	2
99.99998 %	726	4	1	726	4	3

In Table 2 there are illustrated values of possible availability of MTBF and MTTR of one-month devices connected in a row. All values are trendsetting values not real values. In Figure 11 is the formula itself for how to count availability of devices in row.

$$D_t = D_1 * D_2 * D_3$$

Figure 11. Devices in row formula (Metropolia, Cybersecurity program, 2016)

As Table 2 illustrates, devices connected in a row decrease availability. More devices connected in a row the greater chance to loss of availability. This configuration is not recommended in any kind of high availability scenarios.

Table 2. Devices in a Row

SLA	MTBF	MTTR	Failures	uptime	down-time	Devices (in a row)
99,45 %	726	4	1	726	4	1
98,91 %	726	4	1	726	4	2
98,37 %	726	4	1	726	4	3

In Figure 12 devices connected in parallel (left side) and connected in a row (right side). If one of devices is broken the connectivity will be lost completely when devices are connected in row. Devices in parallel by losing one or two devices keep connectivity alive so cause performance decreases if one or more devices are lost.

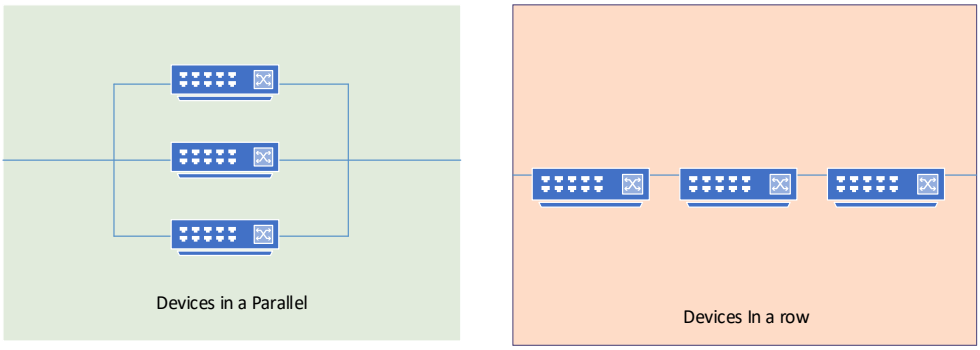

Figure 12. Devices in parallel and Devices in a Row

Devices in parallel can be configured in the load balancing mode. Three devices in parallel in a load balancing mode are recommended. Using failover mode with three devices is waste of money and waste of devices only one device is usable and other devices are passive and idling waiting for an active device failure.

3 Mandatory Processes for Companies

3.1 Disaster Recovery Planning

Disaster Recovery Planning (DRP) is a part of Business Continuity Planning (BCP). DRP scenarios must be designed and tested against vital critical systems in a company. Good and yearly trained recovery plans increase the chance of recovery from disasters and increase companies personnel know-how of disaster scenarios and how to recover from malfunctions. Every critical system necessary to a run business must have recovery plans and many scenarios as possible. When testing disaster recovery scenarios, there must be disaster recovery environment which is like a production environment. There is no need for exact environment. One thing to remember when disaster is ongoing, is communication who can communicate outside of a company and how to proceed when something happens. These communication rules must be clear to everybody in a company.

In the disaster recovery it is good to have backup strategy: how to restore virtual machines, how to restore databases and how to restore systems everyone use every day. A Recovery Time Objective (RTO) means acceptable downtime. The RTO is illustrated

in Figure 13. How long a business can wait for these systems to be back online or in other words when these systems must be back online based on Service Level Agreement (SLA). If this question is asked from company management, the answer is most likely less than an hour downtime is allowed. Figure 13 illustrates Recovery Point Objective (RPO) which means where in time a broken system can be restored. In other words how much data is lost. Where is the latest working backup point the data can be restored to. If SLA is 24 hours, one day back from current time and best restore point that can be used is 12 hours back so that would be in a time frame. Most likely RPO is much less than 24 hours. (https://www.solarwindsmsp.com, 2017 and https://www.druva.com, 2017)

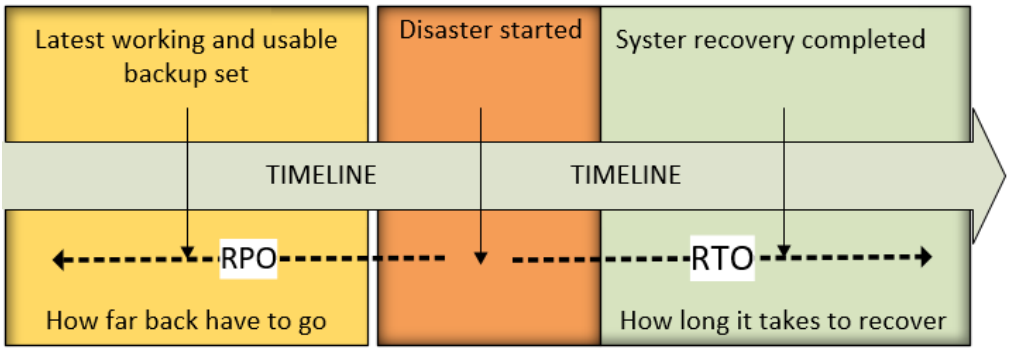

Figure 13. RPO and RTO

How likely certain scenario is going to happen? If the answer is probably never there should be no reason for the recovery scenario. If there is a chance that scenarios sometimes happen, create a plan and good documentary of settings and configuration, who are the key contacts in these scenarios and what installation files are necessary to complete recovery process. Determine impact on the business in certain scenarios if something goes wrong. Determine can people do their work and how much money is lost during a disaster. (https://www.solarwindsmsp.com, 2017 and https://www.druva.com, 2017)

3.2 Change Management

Change management is very important in companies. Example is based on Information Technology Infrastructure Library (ITIL). Company provides a SaaS (Software as a Service) environment to meet customer's needs. Provider makes a change in the system

without properly testing the change and does not inform the customer's stakeholders about the change. Therefor cause malfunction in the system. A service provider can do a rollback, but a rollback has not been tested properly and a SaaS provider might cause long outage for a system customer needs to run daily business. In change management SaaS Company will create a plan for change and propose change for implementation.

One of the key objectives in change management is to minimize downtime by ensuring all changes are planned, documented, tested, authorized, prioritized and implemented.

A change management process is illustrated in Figure 14. The goal of change management is established by policy for handling change requests in an efficient way minimizing risk and downtime in business. (https://www.cherwell.com, 2017)

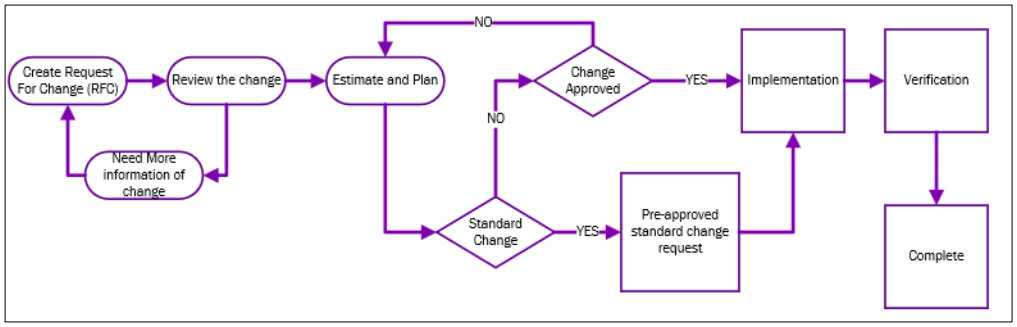

Figure 14. Change management process (https://www.cherwell.com, 2017)

Create Request for Change (RFC)

RFC is commonly done by an architect or other individual who is responsible for the system. First RFC is going to be a draft copy of a document for review. The document must be specific enough and understandable on review. Change can be unapproved and closed. Sometimes more information is required especially when RFC looks promising and mandatory for a business. More information is requested if rollback plan is missing from the document, so prepare RFC carefully before review. (https://www.cherwell.com, 2017)

Approving the RFC

There is standard change which is always auto approved because standard changes are always documented and already tested, these will automatically skip Change Advisory Board (CAB) meetings. When RFC is not standard change RFC has to be approved in a CAB meeting and the RFC reviewed by CAB members on early state of the change. RFC is evaluated how critical RFC is for a company and a risk of increased downtime for a business. (https://www.cherwell.com, 2017)

Implementation and Verification

Once RFC is authorized by a CAB team. Implementation can begin in scheduled time, which is mostly during planned service breaks. After implementation if everything went as planned, service needs to be verified by the testing team. After verification of success implementation RFC will be closed. (https://www.cherwell.com, 2017)

4 Security Controls

Security controls are for minimizing security risks in companies. Security controls help detect, stop and counter security risks as well, when controls are well planned and implemented. Security controls should also determine what needs to be done under certain conditions like when a network is breached, or any other unwanted event is occurring. In the cybersecurity field security controls focus everywhere. Here are introduced Center of Internet Security (CIS) top 5 list of security controls and they all are critical controls. Furthermore, there are 20 controls listed by CIS and they are sorted by importance. The bigger a company is the more controls are most likely implemented to protect against threats. (https://www.cisecurity.org/controls, 2017)

- Inventory of authorized and unauthorized devices
- Inventory of authorized and unauthorized software
- Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers
- Continuous vulnerability assessment and remediation
- Controlled use of administrative privileges

4.1 Inventory of Authorized and Unauthorized Devices

Possible attackers are scanning companies' networks they have targeted by on their own interests or on demand by other party. Whenever new device is added on a network and device has known vulnerabilities attackers may have chance to exploit device. Even if device has no access to internet but network is already breached by an attacker who waits for potential devices to continue attack process and gain persistent foothold on targeted network. There can be new network devices installed in a network which are not properly configured which may allow attacker to do malicious action in a network. When devices are controlled and allowed in a network in controlled way by network administrators these attack possibilities are decreased. In a network should be automated asset inventory discovery software installed and both IPv4 and IPv6 networks should be scanned and most likely DHCP is configured for automatic IP address assignment therefor these assignments must be logged properly. (https://www.cisecurity.org/controls, 2017)

People like BYOD (Bring your Own Device). BYOD can be hazardous to companies networks but if security controls or policies deny employee-owned devices can decrease overall welfare and happiness among employees. A company should have inventory lists of authorized and unauthorized devices and this list must be updated regularly. This requires regular network scanning of devices and this helps to detect malicious devices in a network. IT department can get rid of these hazardous devices. Hazardous devices might enlarge attack surface and jeopardize overall security in companies. The BYOD should be allowed by a company IT department and must be controlled properly.

In a certain point of view every device an employee owns as an example a laptop, a tablet, a cell phone or any kind of IoT (Internet of Things) device are BYOD. A company usually purchases smart phone for their employees. These phones are not properly controlled, and these devices must be listed on the BYOD inventory. BYOD devices must be allowed only on certain WLAN (Wireless Local Area Network) which are for user owned devices. BYOD devices should not be allowed in companies office networks.

4.2 Inventory of Authorized and Unauthorized Software

Plan a list of the authorized software with version information which are required to run in a company network for example what software can be installed on laptop or desktop, what can be installed on servers or in other systems. There might be a list of software for developers and common office workers. These lists must be personalized by role. Developers may need all kind of software for testing and developing new software, their devices should be installed in a more secured network segment. Many software has bugs which can be exploited by attackers and these attackers if they are sophisticated enough, use zero-day-exploits against company to gain foothold in the network. Therefore, most companies do not want to install the latest possible version of software. Unauthorized software list can be every software which is not approved on the authorized software lists. (https://www.cisecurity.org/controls, 2017)

4.3 Secure Configurations for Hardware and Software

When new hardware or software are purchased they are shipped with a default configuration. Hardware and software will work as shipped because manufacturers and resellers want to support ease of use in their products. However, these configurations are not secure enough. Default configurations have for example default credentials, old protocols enabled and unnecessary services. Devices and software with default configuration might be exploitable in their default state. (https://www.cisecurity.org/controls, 2017)

Create standard configurations for devices, software and operating systems. Use standardized images of operating systems with commonly used applications in daily work. Never leave any devices with default configurations and update the firmware if updates are available. Devices are probably shipped with older firmware version. (https://www.cisecurity.org/controls, 2017)

Every device must have company standard configuration configured, where all default passwords have been changed and the SSH (Secure Shell) configured instead of the insecure telnet protocol. Default VLAN (Virtual Local Area Network) should not be used and native VLAN should be reconfigured. Unused switch ports configured in shutdown

state and configured in Black Hole VLAN. The black hole VLAN is the VLAN that is not used in a network and all unknown packets are sent there.

4.4 Continuous Vulnerability Assessment and Remediation

Companies which does not scan their network for vulnerabilities actively have higher change to get their systems compromised. Companies administrators must patch operating systems, software and hardware frequently to keep their network safe. Attackers have at least same information as companies have if zero-day-vulnerability has been found. Use Security Content Automation Protocol (SCAP) validated tools code-based and configuration-based vulnerabilities and good well-known system scanners for scanning entire network. Whenever scan has been completed scanning logs have to be checked and any issues must be fixed based on company policy. (https://www.cisecurity.org/controls, 2017 and https://scap.nist.gov/, 2017)

4.5 Controlled Use of Administrative Privileges

Privilege escalations or misuse of administrative credentials are something what attackers want to achieve. Hijacking an exploitable service which is running as administrator credentials and sometimes a domain administrator account is used for running a service. That is only lazy work from administrators. Many administrators think too much time and effort is consumed on configurations with least privileges, which is bad and dangerous excuse. Minimize privileges, only access necessary systems to complete daily work, which belongs to a role an employee has. Always use the group and role-based administration. Never add individual accounts to computer administrator groups, database servers or to any other service if groups supported. Validate need of administrative privileges from time to time and remove unnecessary access rights. Avoid logging to systems with administrator or root accounts. Use ‘Run as’ in windows and in the Linux systems use sudo when higher privileges are necessary. Similar password for every account might feel clever idea because of easier administration of systems. But that will be hazardous if some accounts are hacked. Always use generated passwords for service accounts and if supported use Active Directory managed service accounts. (https://www.cisecurity.org/controls, 2017)

5 Overview of General Data Protection Regulation

The General Data Protection Regulation (GDPR) is privacy legislation which force any registry holder or data handlers for proper handling of personal data. Personal data protection has been effective long time in Europe, but new GDPR goal is to improve security of individuals and modernize the security of personal data handling process. The regulation is effective on 25.05. 2018. From now on it is not enough that companies comply with law. Companies need to prove they have handled privacy policy requirements in planning and implementation of the service. This regulation is good for any individual and can require huge efforts from companies. If regulation is not complied, companies might lose customers trust. There are two administrative fines if breaking GDPR which is levied is case-by-case and fines are 2 % or up to 10 million € of global turnover whichever is higher or 4 % or up to 20 million € whichever is higher. (https://www.itgovernance.co.uk, 2018)

5.1 Personal Data

Personal data is any kind of information that can be compound to the recognizable person. Personal data is information that can be used to recognize a person indirectly by compounding information to the data stored elsewhere. See examples on Table 3 about what personal data is. Whenever processing data and cannot be sure whether data is personal data or not process data by GDPR rules. (https://www.itgovernance.co.uk, 2018)

Table 3. Examples of personal data

Example of Personal data
Name
Address
E-mail
IP- address
Credit card number
Bonus card

5.2 Data Protection Deviations

Data breaches must be reported within 72 hours to the data protection authority. When a company has become aware of the data breach, it does not matter if the breach is a during weekend or public holiday. (https://www.itgovernance.co.uk, 2018)

5.3 GDPR and Individual Rights

Any organization which handling personal data must be clear and transparent in how data is processed and transferred. Transferring personal data outside of EU is limited. Whenever user approval is required any kind of silent approvals are not accepted. And no pre-ticked boxes are allowed. Any consent can be withdrawn whenever a person wants to. A person has the right to correct inaccurate data and demand erase of personal data stored. The data collected for an example by a police or healthcare or similar authorities. These data cannot be deleted by a request of individuals. (https://www.itgovernance.co.uk, 2018)

6 Physical Security

Protecting hardware against hazards is a remarkable thing to do which might help a company survive against blackouts, brownouts or every hazard related to electricity, against flood, unauthorized access and cooling failures. In a datacenter, there can be too low humidity which can cause static electricity. High humidity can cause corrosion which can damage devices in a company’s datacenter. Even equipment placement is influencing, and access control is mandatory and if possible video surveillance as well.

6.1 Uninterruptible Power Supply

The UPS (Uninterruptible Power Supply) is a device that protects hardware from power loss on a brief time factor and allows controlled shutdown of servers. UPS protects devices from power surges, spikes, blackouts, brownouts and more. Investing on a UPS devices should be done before any hazardous events. Many companies purchase UPS after second hazardous event because they cannot believe that can happen to us.

In a huge datacenter must have backup power as well as dual-path power distribution. When the other power path fails then the other path provide power to the datacenter. This is very expensive, so many datacenters have power generators as backup powers. While backup generators are starting UPS batteries should provide power to the hardware during that time. Doubled power-paths must be capable of handling whole power load through one path when power path failing occurs to avoid overloading of a power system. Backup generators are something which must be tested regularly because will be hazardous if these generators do not start up on power failures. (https://blog.schneider-electric.com, 2017)

6.2 Datacenter Cooling Systems, Temperature and Humidity

Cooling Systems

What is the right and proper cooling system for a company depends on the size of the room where devices are located, a budget, building restrictions like is a building designed for hardware. There are water-based systems and air-based systems. Bigger datacenters most likely use water-based cooling systems as the primary cooling system. If a company is hosting or housing other companies equipment in the datacenter, this cooling system must be high-end model with backup cooling systems. Smaller company with few servers running in own premises might survive with air condition provided by building. The air conditioning system should not throttle outside of business hours in the room where hardware is located. Many business parks slow down air conditioning outside of business hours to save in costs. (http://www.datacenterjournal.com, 2017)

Too much heat will decrease expected life time of hardware and heat is a waste from running devices and waste must carry out from datacenter. It is obvious cooled air needs inputs and heat needs outputs in cooling systems. The cooled air rising from floor and warm air outlet is on the roof of room. Water cooling systems are using air for cooling, but air flow is cooled down with chilly water and there must be good water source nearby. (http://www.datacenterjournal.com, 2017)

Temperature and Humidity

Temperature in hardware room is recommended between 18 ºC - 27 ºC to keep hardware lifetime longer and working as intended by a manufacturer. Monitoring hardware room temperature is highly recommended to improve chance to mitigate potential problems due to temperature changes. Humidity cannot be ignored by IT- personnel. The humidity level must be between 40% - 60 %. If the humidity is less than 40 %, which is too dry can result as a static electricity on hardware. Too high humidity over 60 % starts slow corrosion process on hardware and will cause permanent device failures. Keeping humidity on an appropriate level will increase the hardware lifetime. (https://avtech.com, 2017 and https://serverscheck.com, 2017)

Access Control and Surveillance

Physical access control is mandatory in every company. Access to the datacenter or a single hardware room must be limited to only personnel who must have access to hardware. Persons who requires access to datacenters are from the IT personnel which are responsible of datacenters equipment.

People accessing companies' premises must be surveyed. Authorized people must have identity cards and key tags and usage must be logged where and when a person has entered. Areas with higher security like datacenters should have two-factor authentication like PIN code. What they have (key tag) is first factor and second factor is what they know (PIN code). Huge datacenters should implement video surveillance and mantraps alongside with security guards. (https://www.csoonline.com, 2017 and https://www.sans.org, 2017)

6.3 Location of the Equipment

If a company has hardware in their own premises, a room which is chosen for location of the hardware should look like a common room without windows and it should not be in conspicuous location. Nowadays, in business parks probably do not have rooms designed for hardware. If a room is necessary for a company-owned hardware the room must be changed to suitable for hardware. Sprinklers cannot be fired on minor events

like little overheat. Sprinklers might destroy all hardware in the room if they are fired automatically based on too low baseline values. Rooms where equipment is placed should never have flammable items luring around. Examples of flammable items are cardboards, papers and wood. All flammable items will increase the risk of fire in hardware room. After new hardware arrives, disassemble everything before sending new hardware to the hardware room. (https://www.csoonline.com, 2017 and https://www.sans.org, 2017)

7 Defense of the Network

Four points of defensive cybersecurity, predict, prevent, detect and respond are illustrated in Figure 15. Defensive cyber security is preparing beforehand against threats in a company. Defensive cybersecurity predicts what might happen and where it might happen and builds preventive mechanisms in the network. A few effective ways are use of application locker, properly configured access rights and good endpoint protection software. Detecting if something has penetrated defenses of network and after malware has been detected, which needs to be identified as well. Responding to events are normal forensic procedures before removing the infected machine from a network. (https://www.f-secure.com, 2017)

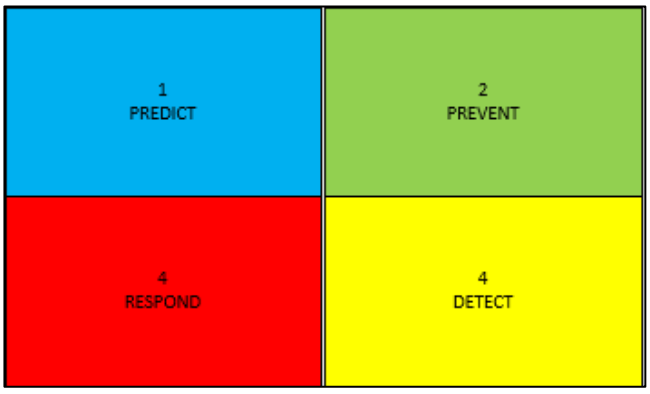

Figure 15. Four points of defensive security (https://www.f-secure.com, 2017)

7.1 Endpoint Protection

An Endpoint Protection (EP) protects companies from malware spreading in all-over the local area network. Therefore, EP products are important and should be installed and configured on every workstation and servers through a management portal. If a single computer is infected by user error or any other way and malware attempts to spread to another system. The EP software attempt stop the spreading of malwares. Some EP software includes Banking Protection. When a bank site is opened, the EP is blocking connections they have nothing to do with bank site communication, which is good feature. Other useful features are web site rating, white and black listing of sites, application control, host-based intrusion detection and prevention and many more. The bigger the company is the better solution with centralized management is necessary. In some small businesses Windows Defender might be good enough and that can be configured through Active Directory (AD).

Gartner defines Endpoint protection as a solution that includes many features such as Antivirus, antispyware, antimalware, firewall, Host-based intrusion detection system (HIDS) in a single product. Endpoint protection attempt to protect against zero-day exploits and many other intrusions as well. A comprehensive Endpoint protection software includes Vulnerability, configuration and patch management through centralized servers. (https://digitalguardian.com, 2017)

7.2 Firewalls

Hardware firewall is the most important security device a company needs. Modern hardware firewall should be placed as the first line of defense. The firewall is protecting Local Area Network (LAN) from Wide Area Network (WAN) in other words from the internet. WAN is collection LANs like Internet Service Providers (ISP) networks, which is illustrated in Figure 16. Many leaders in companies say “Hey, we have the firewall we purchased years ago, our network is safe”, which is not the case anymore. A firewall probably will let sophisticated attackers go through to the network if a user behind the firewall is lured to open a connection for attackers. A Next Generation Firewall (NGFW) is recommended instead of a traditional firewall like SPI (Stateful Packet Inspection). But SPI

and other firewall types are still useful inside networks. There are several different firewall types around but only a few are introduced in this section. (https://metricloop.com, 2018)

- Packet filtering
- Stateful packet inspection
- Software firewall
- Next generation firewall
- Web application firewall

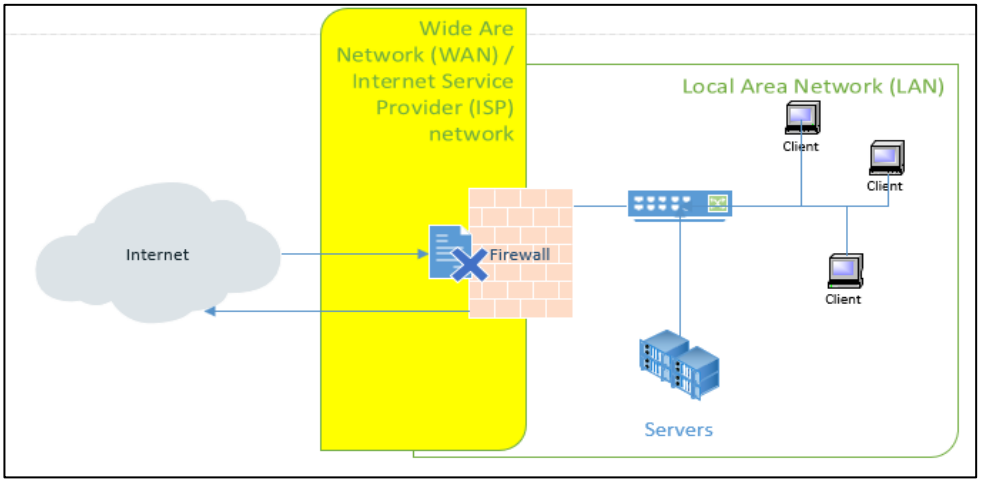

Figure 16. A firewall protecting Local area network

Packet filter

Packet filter firewall can be considered as stateless firewall. Packet filtering firewall watch network traffic very carefully but does not register states of packets. Filtering traffic is based on source or destination, ports or other configured value in firewall rules. (http://www.inetdaemon.com, 2017)

Stateful packet inspection

A Stateful firewall spends most of the time inspecting packet information on OSI (Open Systems Interconnection) layer 4 and on lower layers of OSI model. SPI firewall maintains information of connections in state tables of communication between endpoints and implement security policies and rules configured to firewall. Based on the state of the

packet and whether the packet is participating in any of connections opened by the user behind the firewall decides whether connection is blocked. (http://www.inetdaemon.com, 2017 and http://www.informit.com, 2017)

Software firewall

Software firewall should be installed on each Operating System (OS). Microsoft Windows OS has its built-in software firewall since Windows 7, which is SPI firewall and Linux OS have Iptables, which is packet filter firewall. Even if a network is protected with firewall devices. All computers should have software firewall installed and configured especially on laptops which are most likely used on road. (https://www.linux.fi, 2017 and https://technet.microsoft.com, 2017)

Next Generation Firewalls

The Next Generation Firewalls (NGFW) have built-in security features implemented, not bolted-on features. Built-in features mean security features which are designed in the product to the begin with. Bolted-on features are added later in a product which are added after release and original code of a product is changed. Bolted-on features probably leave some weak points to software. NGFW have threat prevention mechanisms, visibility and control over traffic including encrypted traffic. Nearly everything use encryption in data communication today. Decrypting encrypted data and analyzing data before the data is sent to the end-user help to make sure the communication is normal without any kind of malicious traffic. This does not mean spying of users like what people are doing. This security feature catches malicious traffic on the fly and keeps internet users safe from attacks. Online banking traffic should not be decrypted or any other violating employees' privacy. Before planning any of these connection decryption features within companies, a legal consultation is required. Company personnel must be informed properly what, why and when the IT department is doing. This feature is used to avoid data loss and protect privacy. Paloalto´s NGFW use wildfire cloud-based threat analysis service to identify malicious traffic which is analyzed in a cloud service offered by firewall vendor. (https://www.paloaltonetworks.com, 2017 and https://www.networkworld.com, 2017)

Web Application Firewall

A Web Application Firewall (WAF) is protection for HTTP (Hyper-Text transfer protocol) applications. WAF can protect against XSS (Cross-Site Scripting) and SQL injections and against many other known attacks. A WAF is like a reverse-proxy which monitors, filters and block malicious HTTP traffic based on rules configured. (https://www.owasp.org, 2017)

Future of Firewalls

In the future, firewalls are protecting networks, but more and more cloud-based technology is within firewalls. Firewalls will have more detection methods on traffic and hopefully better chance of separate legitimate and illegitimate traffics and allow only legitimate traffic through the firewall. It is very hard to determine where firewalls are going, they are evolving, and more and more traffic is analyzed in cloud and firewalls must handle super high-speed traffic in the future. At least 10 Gigabytes in a second or even faster traffic. Even network speeds getting faster, and faster firewalls must able to scan traffic for malwares, detect attack attempts and maybe even able protect other hardware within a local area network. Most likely more and traffic will be analyzed in firewall vendor cloud service system. Cloud-based systems will be updated faster, and detection of malicious traffic is better. There is a huge chance that security will increase by cloud-based technologies. Probably configuration of some devices will be in cloud system and that might allow better support from vendor because owner of the device and the account can allow support person to troubleshoot configuration of the device. (https://www.informationweek.com, 2017)

7.3 Intrusion Detection Systems

IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) are not the same. Where IDS is detecting and reporting possible anomalies in the network without stopping bad traffic. The IDS only detecting and informing administrators which is illustrated in Figure 17.

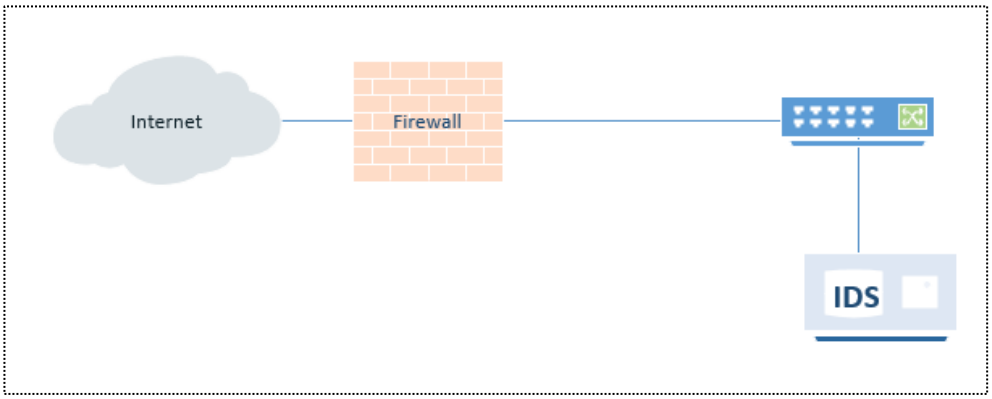

Figure 17. IDS in a network

IPS is detecting, preventing and reporting detected anomalies in a network. The IPS is more complex and requires more attention from administrators. The IPS might block legitimate traffic which is called false positive. Furthermore, the IPS is like a firewall both are installed inline which is illustrated in Figure 18. The IPS is not a firewall and cannot replace a firewall, but IPS can be a security mechanism in addition to a firewall. (http://searchsecurity.techtarget.com, 2017)

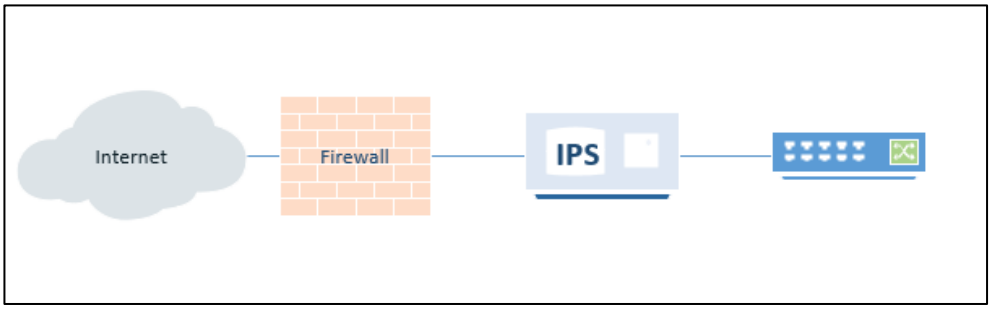

Figure 18. IPS in a network

Many firewalls include IPS or IDS as a built-in feature or bolted-on feature. IPS examines network traffic based on signatures and use heuristic analyses of traffic seeking possible threats and vulnerabilities. The IPS is preventing unwanted traffic by blacklisting sources of malicious traffic. The IPS is always installed inline so only one IPS device is a single point of failure. There are a lot of false positive hits within network traffic. Good configurations are time consuming and own network team should take care of these security devices. The IDS (Intrusion Detection System) works somewhat same way as IPS but IDS do not prevent dataflows. The IDS only sends reports to administrators, informing

misbehaving actions within network traffic. IDS and IPS requires a lot of work and attention from administrators before these devices can be implemented in production networks. Furthermore, these devices cannot be left running somewhere in the network after they are installed they require active administration. (https://www.paloaltonetworks.com, 2017)

7.4 Network Monitoring

Network monitoring is important element in any companies networks. Monitoring network is usually done with software like System center operations manager (SCOM), Nagios, Zabbix and many more. It is critical to know when Virtual machines (VM) are running out of disk or consuming too much disk Input/output (I/O) times, or consuming too much Central Processing Unit (CPU) or Random Access Memory (RAM). A monitoring system can inform if a VM freezes or crashes. Monitoring tools should also have configured to monitor network devices as well to detect failures on time. Monitoring software requires an engineer to monitor and handle events and administrators to create rules what needs to be monitored within network. All servers and network equipment needs to be monitored. (https://www.techopedia.com, 2018)

7.5 Virtual Private Network

Virtual Private Network (VPN) is a solution for securing communication over public network other words over internet. Communication between head office and branch offices are good to handle through Site-To-Site VPN tunnel, which is illustrated in Figure 19. To build direct links from the one office to another is expensive so VPN solution would be cost-effective and secure solution. The Site-To-Site VPN can be used to connect a company network to a customer network. Connectivity is limited to certain services only and customer do not have access to other company's network unless that is agreed to and necessary. Even though the site-to-site VPN is appropriate choice between companies. Many want to use client-based VPN solution which might be more secure from target company point of view and probably even easier to setup if VPN service is already exist in the company. All activity in a VPN tunnel can be logged like who logged in and where that person connected to and when that happened. (https://www.computerworld.com, 2018 and https://www.cisco.com, 2018)

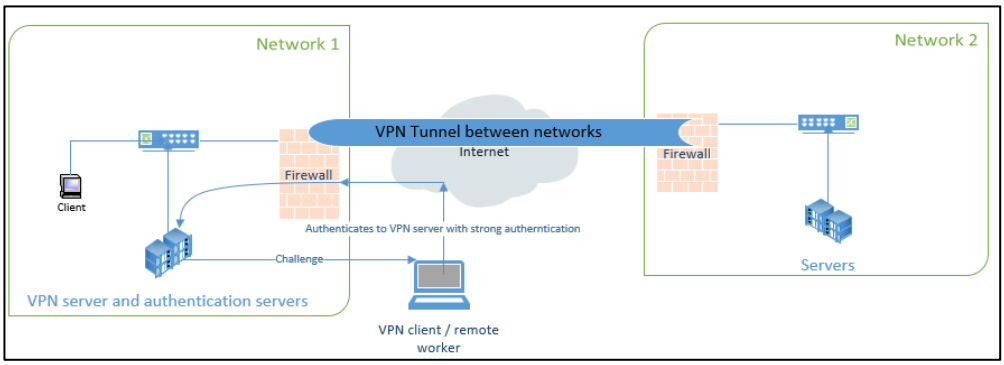

Figure 19. Site-To-Site VPN and VPN Client

Nowadays employees are working remotely. Employees need to connect a company's private network remotely from home through a client-based VPN solution, which is illustrated in Figure 19. The client-based VPN creates secured tunnel between the client and the remote VPN server. A strong authentication is recommended and must be a mandatory requirement when connecting private network remotely to mitigate abuse of private network. This kind of VPN solution allows employees to work securely from hotels when they are traveling and most likely use of VPN solutions makes people feel more secure. (https://www.computerworld.com, 2018, https://www.cisco.com, 2018)

7.6 Wireless Security

Securing WLAN (Wireless Local Area Network) Access points (AP) properly is important. Currently the most secure Wireless encryption is WPA2 (WI-FI Protected Access) even though that too has been cracked. Cracking the WPA2 is not effortless and the WPA2-Enterprise (WPA2-Personal for home users) is best option available. A WEP (Wired Equivalent Privacy) should not be used because it is hackable in the matter of minutes by a moderate skilled attacker. The WPA2-Enterprise have some requirements, which is RADIUS (Remote Authentication Dial in User Service) server. The RADIUS allows authentication through an Active Directory and certificate authentication. A port authentication 802.1x should be implemented. The 802.1x is not only for Wireless security it is solution for wired network as well. A few things that help to increase wireless security are in Table 4. For example, hiding SSID (Service Set Identifier) which only disables broadcasting of WLAN SSID but SSID can be found with reasonable effort by use of a specific application like Aircrack-ng. Many of the attackers will pick up easier targets and

leave hidden networks alone. MAC (Media Access Control) filtering which only allow specified devices to connect wireless network. A MAC address spoofing can fool the device and traffic is allowed through the device. (https://www.sophos.com, 2017 and https://9to5mac.com, 2017 and https://www.sans.org, 2017)

Table 4. Wireless security

Action	usefulness
Do not broadcast SSID	low
Use strongest encryption possible (WPA2-enterprise)	Highest
MAC Address Filtering	Low
Restrict access to WLAN endpoints outside workhours	Moderate
Use 802.1x Authentication	Highest
Patch your Routers and endpoints	Highest

7.7 Centralized User Account Management

Centralized user account management is important. For example all user accounts, group memberships, access rights and group policies can be controlled and managed from centralized location. An ADDS (Active Directory Domain Services) for an example. The Active Directory is scaling from small companies to large corporates. Some alternative directory service solutions are available for an example an Open LDAP (Lightweight Directory Access Protocol), a Red Hat Directory Services. Use of centralized management point and not using local accounts on systems increases overall security drastically. (https://msdn.microsoft.com, 2017 and http://merabheja.com, 2017)

Active Directory

The Active Directory Domain Services (ADDS) is included in Microsoft windows servers and ADDS is designed to manage and administer Windows clients networks. The ADDS umbrella offers usable services such as Certificate Services, Federation services, Rights management. The Active Directory is for managing and administering domains, User objects, and computer objects within a forest. Active Directory logs every user logged in a domain and authenticates and authorizes accounts in the domain network. Active Directory allows administrators to configure various group policy objects to user accounts and computer accounts based on filters such as group memberships and WMI (Windows Management Instrumentation). The ADDS have DNS (Domain Name System) integrated

zones, which are replicated with the ADDS replication. Writeable ADDS servers in the domain have writeable DNS servers if DNS feature is installed, which means the integrated DNS is multi-master like the ADDS. (https://techterms.com, 2017 and https://technet.microsoft.com, 2017)

Alternative Directory Services

There are alternative directory systems available but, in Windows networks Active Directory is best and probably most secure solution available. The Red Hat Directory server is for UNIX environments. Open LDAP is open source application, which is Windows LDAP client and probably one of the best alternative for Microsoft Active Directory. In medium size or larger Windows networks the Active Directory is recommended. If use of open source system is desirable, there is no official support available and fixing issues might get harder if there are no advanced know-how of these system. (http://merabheja.com, 2017)

An alternative for smaller networks would be a Network Information System (NIS). A NIS+ is improved version of the NIS which has more security features. The NIS is developed by Sun Microsystems, which is now owned by Oracle. The NIS is like a DNS, but it is designed for small networks and will not be effective solution for medium size or larger networks. NIS provides a username with password login mechanism which allows access on many hosts with the same user credential. The NIS code has been released for public domain and there might be more alternative version available in the future. (http://searchnetworking.techtarget.com, 2018 and https://docs.oracle.com, 2018)

Network device authentication

Authenticating to many network devices by using a local username on device will be hazardous. A network device authentication can be handled through Active Directory with the RADIUS (Remote Authentication Dial-In User Service) server, which can handle Authentication, Authorization and Accounting (AAA). The RADIUS authentication and authorization is accepted if a username and a password values are correct. Although Diameter is replacing RADIUS in the future. (http://www.ciscozine.com, 2018 and https://www.tutorialspoint.com, 2018)

Securing network physical access is easier when an administrator can control, which devices can connect to the network. This means an attacker needs physical access to a device which has access to the network. A port authentication 802.1x, which is mostly used in WLAN networks, but many companies are implementing 802.1x to LAN switches, which is appropriate solution. The 802.1x use MAC address databases. MAC addresses and IP (Internet Protocol) addresses can be spoofed. The spoofing can allow man-in-the-middle type of attacks against a network. Preventing the man-in-the-middle on 802.1x implemented combine an Extensible Authentication Protocol (EAP) to authenticate client to the network. There can be used certificate or a username and password or combination of both with the EAP. After an authentication is completed, a system assume all traffic is legitimate traffic. Security can be increased by implementing an Internet Protocol Security (IPsec) for encrypting end-to-end traffic. Since Windows Vista and Windows server 2008 R2, Microsoft introduced a Network Access Protection (NAP) technology, which protect network against unhealthy devices based on rules an administrator implemented to the network. (http://searchitchannel.techtarget.com, 2018 and http://searchitchannel.techtarget.com, 2018)

7.8 Data Loss Prevention

Data Loss Prevention (DLP) is a protection strategy to ensure sensitive data is not accessed by unauthorized users and prevent data loss. DLP software products can classify data by sensitiveness and mark data for example critical, confidential and company confidential. A DLP can prevent sharing data accidentally or sharing data on malicious means. A DLP software can monitor endpoint activities and filter data. Possible threats inside a company and probably laws are increasing demand of DLP software in companies to avoid of sensitive data leaks. DLP solutions are good but might be laborious on start implementing DLP on scratch. (http://whatis.techtarget.com, 2018 and https://digitalguardian.com, 2018)

7.9 Documentation

Everything needs to be documented. A company has several critical systems online and a company has a disaster and a bunch of servers goes down. If there are no documentaries what was installed on servers and what was the actual purpose of servers. It is

hard to get servers back online fast enough as they were before disaster. All server and network device information should be documented well enough and all configuration they have needs to be documented. Document everything and update the documentation in the yearly reviews.

7.10 Employee Training

Security and awareness training of employees should be done at least twice a year. Another training event can be something where all incidents inside a company are introduced to employees anonymously and current security threats introduced to employees what has happened elsewhere in the world. Another event can be reminders why the cybersecurity precautions are being made in the company. There are so many employees who think these controls and policies are written to bully employees. Train employees and write justification of every security control and policy a company has and promote how these controls and policies protect privacy of employees and protect a company's vital information such as trade secrets.

7.11 Security Audit and Security Scanning

Security audit

A security audit is not a security scanning or penetration test, which should not to be confused with them. Security auditing is about determining if company's server configuration, network devices or any other security measure are complying with standards, best practices or with legislation. A security scanning can be used as a tool for audits to get better evaluation of a system state in audit process. A company who will do audit will write a complete report what is configured wrong and what is good in the system they are auditing. Which means is a system complied either best practice, standard or legislation and which of them are not complied.

Security scanning

A security scan, which can be a service provided by cybersecurity companies or a company can have own security scanning servers installed. The security scanning is useful because vulnerabilities can be found from a scanned network. The security scanning report help to mitigate security issues in the network. There will be a lot of false positives in scanning reports. Security scannings should be done periodically and fix security issues scanner found during a scan process. A scoring is based on the Common Vulnerability Scoring System (CVSS). Everything cannot be fixed, but all scored over seven should be fixed, because these can be exploited more easily and that can cause serious harm to a company's business. The CVSS score less than seven should not be ignored. All of these has to be checked and fixed if that is necessary based on how critical environment is and what kind of vulnerability is found. The CVSS scoring is illustrated in Table 5. (https://scap.nist.gov, 2017 and https://www.sans.org, 2017)

Table 5. Common Vulnerability Scoring System (https://nvd.nist.gov, 2017)

Severity	CVSS score
Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 – 6.9
Low	0.1 - 3.9
None	0.0

7.12 SIM, SEM, SIEM

The importance of log management is growing all the time especially after General Data Protection Regulation (GDPR) launched in European Union (EU). A user actions must be trackable from log management system like how, when and where an unauthorized access to the network has occurred or any kind of Information disclosure has occurred in the network.

Security Information Management (SIM)

A SIM is collecting, monitoring and analyzing data of computers logs and from devices for example firewalls, IPS and IDS devices. The SIM is correlating collected logs in readable format and provides security reporting and analysis of the collected data. These systems collect a huge amount of data, which is collected to a secure location and in read only mode. The SIM based products are good for log management. Collected data consumes easily up to 10 terabytes storage in a midsize company. The SIM is easier to manage and deploy than a Security Event Management (SEM) and SIM systems requires less effort from administrators. (https://www.symantec.com, 2017 and https://www.techopedia.com, 2017)

Security Event Management (SEM)

A SEM is strong on event management and in real-time threat analysis. SEM products are not as good for log management as SIM systems are. The SEM can give good visualization of events and help on incident response. SEM systems are harder to configure than SIM systems. SEM systems are complex and time consuming from administrators point of view and require daily work for keeping systems running effectively. (https://www.symantec.com, 2017 and https://www.techopedia.com, 2017)

Security Information and Event Management (SIEM)

SIEM systems are a combination of the SIM and the SEM systems. SIEM systems offer real-time analysis of alerts and real-time threat analysis. SIEM systems can read for an example syslogs, windows event logs, actually nearly any kind of text-based logs. Any non-standard logs need to explain to the system how to read them. A syslog does not have standard how they should be written, which means an administrator has to instruct the system how to read a log file every time a new log format is collected. The SIEM collecting a lot of log data, which going to grow huge on a storage system consuming over 10 terabytes up to 100 terabytes. These logs need to hold in the safe location 2 – 10 years depending of log type and industry. SIEM systems can find anomalies from logs it is collecting. These rules need to be configured to the system or learnt by the system. The SIEM is very hard to configure and requires full duty administrator and probably

consultation from SIEM specialist at the start of the SIEM project. (https://www.symantec.com, 2017 and https://www.techopedia.com, 2017)

Correlation and analysis of collected logs

These systems SIEM, SIM and SEM fetch logs from systems where a system is configured to do so. Analyzing collected logs is time consuming. An administrator must know what to search for, not specifically but for an example when something has happened. These systems can correlate events based on rules and show anomalies on dashboards configured to systems. Timestamps are critical, all clocks need to be synchronized on systems participating in log collection. Collected events must be able to prove what has happened, when it happened and how that happened. When collecting events, all noise should be filtered out, but if cannot be sure what the noise is, it is safer to collect everything. Analysis of logs must start on demand or when a system raises alert of anomalies in the network because nobody wants to violate a privacy of others. Furthermore, all systems need to be logged for example firewalls, load balancers, routers and servers. It is critical that administrators or forensics specialist can trackback where, when and how attackers breached the network. Correlation of logs is mandatory and there cannot be blind spots when tracking what has happened, when it happened and where it happened. These logs collected must be undeniable evidence in the court when requested by officers.

8 Network Threats

Many companies today provide services online. A DDOS (Denial of Service) is big and growing problem to companies, because DDOS attacks are interfering offered services, which can only be a bluff to cover actual attacks against a company. Data breaches are a big problem for every company. If a data breach happens, companies have for an example employee information, trade secrets, credit card numbers and customer information. Information companies have attackers can sell information in the black market or use information for hindering target companies reputation. Attackers can target attacks to payment systems to make money transfers unstable, which may cause financial setbacks to companies and to common people. Attackers want to do this for fame and glory

in their own communities, political views, disliking decisions made in companies or just for fun.

8.1 Proactive Reaction to Threats

Any company should react on threats before anything bad happens by protecting valuable assets with necessary security measures. This means proactively approach on threats before anything bad happens. There must be written security policies how to react when attackers attempts to breach the network. When attackers have breached the network or when suspecting possible ongoing attack in a network can be very expensive. Protecting the network proactively might save a lot of money, if upcoming network breach can be blocked right at the beginning of an attack. There is a huge change that a company IT department does not even know of ongoing breach to company's network. It is possible the attack is persistent and has been effective long time in the network. An important thing is to understand that most likely attackers who want to breach the network will bypass firewalls. If everything is configured properly and everything has been patched, attackers probably cannot get any foothold in systems without huge effort.

8.2 Critical infrastructures

If a company is in a critical sector for an example energy or healthcare sector, losing electricity on large area or if health care information is compromised would be quite bad for everybody and these must be protected.

Energy sector

Energy sector use SCADA (Supervisory Control and Data Acquisition) systems. SCADA might be most important system in an energy sector, which must be protected at all cost to avoid unauthorized people accessing system. One well known attack against SCADA was STUXNET malware. The malware was probably by Israel-American made against Iranian nuclear program. Stuxnet falsified all monitoring information of centrifuges and allowed attackers to control rotation speeds from slow to fast and fast to slow very rapidly to destroy centrifuges, which caused severe damage to the systems. That was closed

system with no connection to the internet at all. An infected USB (Universal Serial Bus) memory sticks was planted around the facility. An employee of nuclear plant attached infected USB stick to a computer the worker used for daily work. (https://www.symantec.com, 2017)

Another attack against energy sector is Ukrainian power grid hack which happened during winter at 2015. The attack against power grid was discovered by an employee who was finishing a day at work. The worker noticed a mouse cursor moving on the screen. Attackers start controlling circuit breakers at a substation and on a pop-up dialogue message attackers clicked confirm. The substation went down leaving thousands of residents without power. All lights and heaters went down, basically everything which needs electricity. An operator tried to stop what was happening, but all the operator tried was unsuccessful. Attackers logged the user out from systems and changed password of accounts they used preventing re-logging in to the systems. (https://www.wired.com, 2018)

After all, attackers took about 30 substations offline, leaving over 230 000 people without power. Attackers also launched a Telephone Denial of Service (TDOS) attack to the customer call centers to flood bogus calls to prevent legitimate calls from getting through. Attackers also disabled backup power systems of two out of three distribution centers to ensure operators are in the dark and cannot do anything to help in ongoing problematic situation. The attack was sophisticated and well-funded. Most likely the attack started over six months earlier than actual power grid shutdowns. Ukrainian power grid systems were well protected with multiple firewalls, network segmentations and good logging to allow security experts to reconstruct events of the attack. They did not use two-factor authentication which allowed attackers to hijack credentials and gain access to SCADA systems. (https://www.wired.com, 2018)

Attackers wrote malware which overwritten multiple systems firmware on many substations leaving systems in malfunctioning state. The attack started with spear-phishing campaign against IT employees. Attackers used malicious macro code attack, a word document attached to well-crafted email. An IT employee opened the attached document which asked to enable macros, by enabling macros infected their systems with BlackEnergy3 variants and opened a backdoor to attackers. The attack required lots of patient and funds during reconnaissance how to orchestrate successful attacks against power grids. (https://www.wired.com, 2018)

Healthcare

Many healthcare sector systems require fast accessibility for an example patient monitoring systems. Patient monitoring systems cannot be used with strong authentication because every second might matter when saving patients lives. These devices must be secured another way. No unauthorized personnel allowed in rooms and protect device sockets proper way. No one cannot plug anything in devices, all writeable ports must be protected carefully. Many devices still use old and vulnerable Web Equivalent Privacy (WEP) or another less secure way to connect devices. Many devices do not support WPA2 protection because of hardware restrictions. Devices like pace makers or insulin pumps are so small and complex, which makes impossible to get enough memory inside devices to meet WPA2 protection requirements. Devices must have chance for remote management for better control and monitoring. Everything evolves, better and smaller hardware can be built on a smaller surface, which makes better security possible in the future. Healthcare devices cannot be patched easily. If there are bugs in devices operating systems and devices do not have good update strategy and no update servers available from vendors. Probably many devices have old firmware installed because it is impossible call back every device. When time passes devices might be more vulnerable and device vendors do not support devices if configuration has been changed. Probably many devices are not updated at all because of this restriction. (https://www.sans.org, 2017 and https://www.forbes.com, 2017)

Many hospitals personnel do not have knowledge and skill to update medical devices. Even though if they have skilled people with knowledge, how to secure devices against of misuse. Hospitals may lose warranty of devices because vendor has restricted device modifications. Manufacturers of healthcare devices are very slow with security patching. Many of these healthcare devices are old and use old unsupported operating systems, which many of devices are insecure since birth. Manufacturers might restrict of installing third party endpoint-protection (EP) software on devices. EP software can cause harm to the device and device might become unresponsive or less accurate. Most likely device manufacturers recognize these security problems and adding security in design method on new device models. Many hospitals still have old devices installed in their network and insecure device might allow attackers to breach hospitals network. The biggest fear is someone could remotely cause harm to the patient, by falsify the data output of device and force wrong treatment to the patient. (https://www.hpe.com, 2018)

There was a huge ransomware attack against healthcare in 2017 where attackers used wanaCryptor 2 or WannaCry against the NHS (National Health Service). Attackers malware, which exploited windows operating systems vulnerability. Microsoft already fixed vulnerability in March 2017. In December of 2017 was reported operating systems they used was old Windows XP and Microsoft stopped providing patches for Windows XP operating system in year 2014 and still NHS did not upgrade operating systems. This attack spread out in many countries in Europe. Later attack spread in United States and South America. A group called Shadow Brokers, which claimed they have stolen some Cyber Weapons from National Security Agency (NSA). There was skepticism if they are able to do hack against the NSA. Cyber weapon (malware) was used in this attack to spread ransomware all-over the world. Ransomware encrypts the user data and send payment request to victims for decryption key. Sometimes when ransom is paid, they may never send actual decryption key or there is a chance that the key does not work. Ransomware is growing as a threat all over the world. (https://www.theguardian.com, 2018)

8.3 Data Breaches

A data beach is an incident where a company's valuable and sensitive data has been compromised by unauthorized users. The data breach can be data theft, data has been read by an unauthorized users or data has been tampered. A data which has been breached can be for an example trade secrets, list of customers, healthcare information, personnel information or anything which can be adverse to the business. A data breach is not always caused by external threat. This can be an employee who read an unauthorized data, which employee should not have access rights to. Good example is healthcare, unauthorized hospital employee read a patient information from a computer. The employee does not have authorization, this can be an accidental or purpose. All data regarding privacy must be protected properly. (http://searchsecurity.techtarget.com)

8.4 Reconnaissance

A reconnaissance is where attackers start malicious actions. A classic way is to bring many infected USB memory sticks to a conference masqueraded as a carrier services worker, who asks a signature from a receptionist to confirm that these were ordered to

the conference. Probably someone will use a USB stick and attackers may have a completed first step of the reconnaissance process.

A benevolence of people is something attackers want to use against a company defenses. Simply calling to the target company and ask some information like who is responsible Information and Communication Technology (ICT) infrastructure and probably gain information of subordinates as well.

The reconnaissance can start on company's websites or job advertisements. Hopefully get information of systems the company is using in their infrastructure and attackers may find possible weak spots from the network. If attackers can lure access rights to network by impersonating as a company employee and helpful helpdesk person resets password for attackers. Reconnaissance is simply way to get information from possible target company to make breaching the network easier and effortless.

8.5 Advanced Persistent Threats

Advanced Persistent Threats (APT) is an attack method where attackers gain unauthorized access to the network they have targeted, and attackers stay there an extended period. Companies which have valuable information in their network, attackers can use on their own benefits most likely selling to other parties like competitors on same field of business. Attackers want to get in the network undetected as fast as possible and get out as fast as possible without leaving any tracks of unauthorized visit in a network. Attacker avoid defenses such as IDS and IPS systems. In APT attackers need to maintain unauthorized access to a network. If the network does not have any defenses attackers can stay and maintain unauthorized access to the network they have targeted. Assumed the network have good defenses against malicious actions, therefore attackers need to rewrite attack codes for evasion of defensive systems in the network. Well-built defenses increase change of mistakes by attackers and leave some tracks where and how they breached the network. (http://searchsecurity.techtarget.com, 2017)

Attackers may have access to the network, but they need to have valid credentials for access to network resources. A social engineering is a key for attackers. Probably a spear phishing technique is used against carefully selected employee in a company who

has authorized access to the part of the network attackers are targeting. A probably spear phishing target has administrative access to servers, which would be disservice to attackers. With administrative access attackers can install a backdoor to the network. This means well coded malware which they are installing to the system. With backdoor access attackers can steal information from the network until their plan is mitigated or attackers complete their attack. These types of attacks are hard to detect and difficult to identify. Most likely data theft cannot be completely invisible and most likely attackers cleaned up their tracks well enough. (http://searchsecurity.techtarget.com, 2017)

8.6 Denial of Service

Denial of Service attack (DOS) and Distributed Denial of service Attack (DDOS) are events where attackers want to prevent legitimate users from accessing resources. DDOS attacks can be decoys, which hide attackers' true purpose such as data theft from the network, while network administrators investigate an ongoing DDOS attack. DOS attack types overwhelming resources of servers to make impossible to use services, which is illustrated in Figure 20. The DDOS case is always adverse and needs to be mitigated as fast as possible. Work together with Internet Service Provider (ISP) to block networks where attacks are coming from. If possible filter malicious traffic and allow only legitimate traffic through to the network. DOS attacks might be simpler because there is only one source after it is found, which can be blocked easier with ISP help. DDOS attacks are distributed and have a control host somewhere hidden on the internet, which controls botnet hosts. If the controller can be found and blocked, attacks can be stopped because their commander is offline. But nothing cannot prevent attackers from changing location of controller logically or physically. (http://searchsecurity.techtarget.com, 2017)

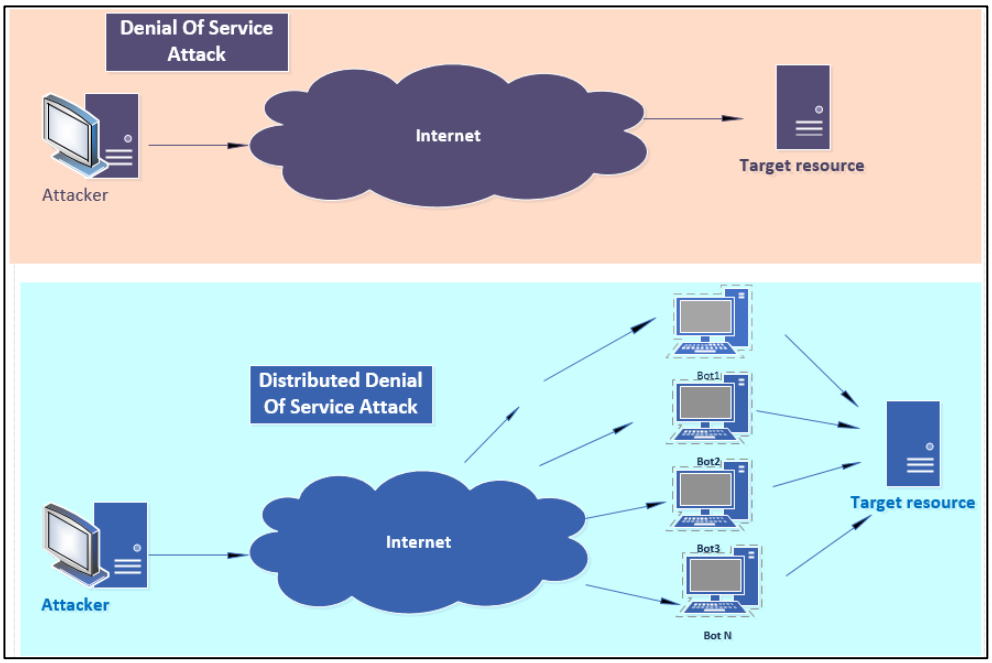

Figure 20. DOS and DDOS attacks

8.7 Ransomware

A ransomware is typically a trojan and victims are lured to download ransomware on a computer. Trojan encrypts victims data and demand a ransom for the victim files usually number of bitcoins. Whether victim pays ransom or not a victim may still lose all the data because attackers do not want to send decryption keys to their victims. When victims' resources have been exploited, a victim is usually notified of the exploit and instructions are given how to recover from attack. There can be many ways to get infected for example there might be compromised websites, infected software or infected external storage Medias. Ransomware encrypts all files it has access to write permission for example in file shares, victims computer or cloud storage. Therefore, it is important to carefully design access rights policies in companies. This is not only a problem of companies, this if problematic for everybody. (http://searchsecurity.techtarget.com, 2017)

9 Mitigation of Many Threats

Mitigating threats is not only hardware or software, which can be bought but they help as well patching them regularly. Security policies and proactive attitude can help mitigate

threats beforehand. Many company leaders have said we are not interesting company nothing bad will happen our business. That is not true, these can be happening to every company in the world. Someone might do something just for fun against a company.

9.1 Patch Operating Systems and Utilities

Keeping all operating systems and installed software up to date in a network with scheduled patching method. There can be used centralized software like System Center Configuration Manager (SCCM), although SCCM might be too heavy for small companies. An alternative method can be used, which needs to be solved by IT service provider. When a new hotfix is released against a threat these hotfixes or patches should be installed as soon as possible. It is recommended to install patches to test environment first to ensure patches itself won't cause any issues to system. Hotfixes and updates to windows operating systems can be pushed using SCCM or Windows Update Services. If there are older operating systems installed in a network and these cannot be updated because of a legacy software. No updates available anymore, after end of vendors maintenance period. These systems must be moved to separate network without connectivity to the office network. By patching operating systems and software installed to systems helps to mitigate exploits of software's installed in the network and make attacks against network harder. There is no way to be sure by patching all software would stop running malicious code after opening document with malicious code. Training employees to be more aware what might happen if malicious code is allowed to run what might cause to the network security. Instructing employees not to run macro codes or other malicious codes and not to open any documents they cannot recognize. For example, must be known sender, email content and sender email must be valid. If an employee even a little bit feels this is not a legitimate email that should be reported to the company security department and let them investigate further.

9.2 Patch Hardwares Firmware

Updating devices firmware whenever new updates are available, there are fixes against exploitable weakness. These firmware updates should be tested first to avoid possible malfunctioning of devices in production environment. There must be rollback plan if devices start failing after an update. There can be many kind of Internet of Things (IoT)

devices and embedded devices, which requires patching as well. The older the IoT device is probably more insecure that device might be, because of security in design was not fashion in the beginning of time in IoT.

9.3 Unknown Peripherals

Peripherals such as USB (Universal Serial Bus) memories or other memory devices are planted all over near of the target company. These can contain malicious code and employee might not even notice what happened when contaminated memory device is plugged in a computer. That USB memory might look empty, but something already installed in the operating system as a process which allow a backdoor access to attackers. The Iranian STUXNET issue, which could have been mitigated, if employees would not have been installed USB stick to the computer, which infected SCADA systems. Maybe, because never cannot be sure if spying agent was working there and infected systems on purpose. If using of USB memories would have been blocked by Windows operating systems group policy might have prevented infections. (https://prajwaldesai.com, 2018)

9.4 Two-factor Authentication

In the Ukrainian power grid hack, they did not have a two-factor authentication in use, which would have been slowed down or minimized damage in the power plant. The two-factor is something one has and something one knows. For example, a password and a username is something one knows and then there are a pin code and a challenge, which is sent to a mobile phone, which is something one has. The two-factor authentication makes nearly impossible to hack user accounts. Yes, nearly there are always something that might go wrong.

9.5 Change Default Configurations of Devices

Changing default usernames and passwords from devices in a network will mitigate or hampers hacking attempts to network devices. Some attack attempts are using device default passwords and if default password is changed this kind of attacks are mitigated.

This needs to be included in policies, which describes no devices with default configuration cannot be installed in the network.

9.6 Endpoint Protection Software Installed

Endpoint protection software installed on every system possible help detecting and stopping possible malware in the network and prevent malware infections on devices and operating systems. Awareness trainings to employees about malwares and security policies, which describes like no administrative privileges on company's laptops and administrative privileges only on systems which are necessary. Endpoint protection software do the best it can, but user awareness and good company policies are necessary.

9.7 E-mails, Attachments and Links

Whenever an e-mail is received, is it from known person or from an unknown. Awareness of what can happen when open unknown e-mail, clicking that link inside an e-mail or opening attachment in an e-email. Employee clicks link or opens an attachment might install ransomware or install backdoor software (Trojan) to local computer. Ransomware start encrypting everything possible inside the network where employee can access with write permissions. The backdoor software can open way to attackers through the firewall. Avoid clicking links before checking them out carefully and be careful with attachments inside an e-mail.

10 Conclusions

The aim of the thesis was to investigate cybersecurity to help others to understand cybersecurity. The thesis helps people to increase their cybersecurity awareness and knowledge which can make people more familiar with the cybersecurity area. This is just a scratch on the surface. The cybersecurity area is huge and contains nearly everything that can be hacked, including human beings. The cybersecurity is a growing and critical component in companies and to common people. The importance of cybersecurity is growing all the time as more and more threats appear from nowhere, luring people to do against their will.

This thesis writing process made me think more deeply about the importance of security controls and security policies. Many people in companies or in communities can find this thesis useful when designing security policies to companies. The thesis does not cover everything in the cybersecurity field. Get more information from the internet and use the reference list for full articles to gain more information on topics in the thesis. Furthermore, a journey on the cybersecurity field can start here and let's make the world more secure.

In the future need to forget the traditional way to protect assets, fortress defenses the only way to protect valuable assets. For example, best firewalls, hardened operating systems, IPS and IDS systems. These systems help but it is not enough anymore. All yearly awareness and security training helps. Being ignorant like that cannot happen to us can be hazardous. When asking from company leaders have the network been breached. Most likely answer is not our network, there are good defenses. When someone breaches the network and is able to create persistent foothold in the network without detection. When breach is detected how much valuable data has been leaked out from the network. The bad guys have the same tools as the good guys have. There is law and good guys cannot break a law without consequences, but bad guys do not care whether they break a law or not. Attacking is most likely easier task to do than defending against attacks.

An Artificial Intelligence (AI) such as machine learning. AI might be only way to detect and stop attacks right away in the future. When machine learning can define what is normal traffic and what is not, that will be a huge defense mechanism in a network. AI can detect whatever anomalies in real time from traffic flow and stop that traffic flow right away. Current problem is when investigating attacks or found a breach, the breach already happened. Currently forensics teams and administrators are investigating breach which already happened but if machine learning will work someday and there is chance investigating when attacks are starting, and attacks can be mitigated right away. An average attack lasts about 200 days, too much valuable information can be lost during the year or in a longer period of time. A competitor might be one step ahead all the time because of this attack they might have ordered or just found a way to buy information from the party launched this kind of attack. (https://www.wired.com, 2018)

if an AI can detect, report and self-configure networks to mitigate attacks. The AI could patch vulnerable systems and reconfigure some parts of network if something bad happens and AI isolates problem away from core services. If machine learning techniques left to make all decisions, then some at point something bad happens. System blocks wrong traffic especially if attackers can lure the system reconfigure network parts or shutdown systems. Every big decision needs to be controlled by a human at least at the beginning. (https://www.eda.europa.eu, 2018)

Complex passwords are hard to remember. Password phrases are easier to remember but can be forgotten and people write them down on sticky notes. Most likely in the near future passwords will be history, not completely but are probably partially replaced by biometric authentication systems. Face reorganization can be used with iris scanning, retina scanning, fingerprints, voice recognition or behavioral biometrics such as keystroke metrics. Most people use pattern or fingerprint when logging into a smart phone or home laptop. Many companies use fingerprint print sensors. If iris, retina or fingerprint data is stolen and data can be used to fool systems to open doors to uninvited persons. Stealing someone's credential is easier than tricking systems in the future. The near future devices used for scanning biometric data are probably super accurate, fooling them might be hard. Authentications and authorizations will be based on who person is by stored biometric data samples. Authentication will not go nowhere, it is evolving little bit. (http://www.directivecommunications.com, 2018 and http://searchsecurity.techtarget.com, 2018)

References

https://software-security.sans.org. 2018. SWAT. [Referred 14.02.2018]
https://software-security.sans.org/resources/swat

https://www.abbreviations.com. 2018. SWAT stands for. [Referred 14.02.2018]
https://www.abbreviations.com/S.W.A.T

http://www.castsoftware.com. 2018. Risk management in software development. [Referred 14.02.2018]
http://www.castsoftware.com/research-labs/risk-management-in-software-development-and-software-engineering-projects

https://www.ietf.org. 2018. IETF RFC. [Referred 09.02.2018]
https://www.ietf.org/standards/rfcs/

https://wiki.en.it-processmaps.com. 2018. ITIL RFC. [Referred 09.02.2018]
https://wiki.en.it-processmaps.com/index.php/ITIL_Glossary/_ITIL_Terms_R

http://searchsecurity.techtarget.com. 2018. MAC. [Referred 09.02.2018]
http://searchsecurity.techtarget.com/definition/mandatory-access-control-MAC

https://www.techopedia.com, 2018. MAC address. [Referred 09.02.2018]
https://www.techopedia.com/definition/25059/media-access-control-mac

http://whatis.techtarget.com. 2017. CIA model and CIA Triad. [Referred 10.09.2017]
http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

https://www.globalsign.com. 2018. Algorithms. [Referred 02.02.2018]
https://www.globalsign.com/en/blog/glossary-of-cryptographic-algorithms/

https://www.globalsign.com. 2018. TLS and SSL. [Referred 08.02.2018]
https://www.globalsign.com/en/blog/ssl-vs-tls-difference/)

https://www.securityfocus.com. 2018. MD5. [Referred 08.02.2018]
https://www.securityfocus.com/bid/11849/discuss

https://www.computerworld.com. 2018. SHA1. [Referred 08.01.2018]
https://www.computerworld.com/article/3173616/security/the-sha1-hash-function-is-now-completely-unsafe.html

http://blogs.getcertifiedgetahead.com. 2018. HMAC. [Referred 12.02.2018]
http://blogs.getcertifiedgetahead.com/hash-based-message-authentication-code/

https://www.cisco.com. 2018. VPN. [Referred 08.01.2018]
https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

https://www.computerworld.com. VPN. [Referred 16.01.2018]
https://www.computerworld.com/article/3184651/networking/5-ways-your-company-can-benefit-from-using-a-vpn.html

https://www.wired.com. 2018. HTTPS. [Referred 10.01.2018]
https://www.wired.com/2016/03/https-adoption-google-report/

http://searchsecurity.techtarget.com. 2017. Integrity. [Referred 11.12.2017]
http://searchsecurity.techtarget.com/answer/How-MAC-and-HMAC-use-hash-function-encryption-for-authentication

http://www.pearsonitcertification.com. 2017. CIA model. [Referred 10.09.2017]
http://www.pearsonitcertification.com/articles/article.aspx?p=1708668

http://world-class-manufacturing.com. 2017. MTBF [Referred 12.09.2017]
http://world-class-manufacturing.com/KPI/mtbf.html

Metropolia, Cybersecurity program. 2016. MTBF. MTTR. [Referred 12.09.2017]
Study material of metropolia cybersecurity program

https://www.solarwindsmsp.com. 2017 Disaster Recovery. [20.11.2017]
https://www.solarwindsmsp.com/blog/5-questions-to-ask-yourself-when-planning-a-disaster-recovery-scenario

https://www.druva.com. 2017. Disaster Recovery. [20.11.2017]
https://www.druva.com/blog/understanding-rpo-and-rto/

https://www.cherwell.com. Change management. [Referred 05.11.2017]
https://www.cherwell.com/products/it-service-management/itil-processes/essential-guide-to-itil-change-management

https://www.f-secure.com. 2017. Defensive cybersecurity. [Referred 15.09.2017]
https://www.f-secure.com/en/web/business_global/our-approach/live-security

https://www.cisecurity.org. Security controls. [Referred 28.11.2017]
https://www.cisecurity.org/controls

https://nvd.nist.gov/scap/. 2017. Security controls. [Referred 28.11.2017]
https://nvd.nist.gov/scap/validated-tools

https://digitalguardian.com. 2017 [Referred 16.09.2017]
https://digitalguardian.com/blog/what-endpoint-protection-data-protection-101

http://www.inetdaemon.com. 2017. Stateful and stateless firewall. [Referred 28.10.2017]
http://www.inetdaemon.com/tutorials/information_security/devices/firewalls/stateful_vs_stateless_firewalls.shtml

https://metricloop.com. 2018. LAN and WAN. [Referred 27.01.2018]
https://metricloop.com/library/network

http://whatis.techtarget.com. 2018. DLP. [Referred 14.02.2018]
http://whatis.techtarget.com/definition/data-loss-prevention-DLP

https://digitalguardian.com. 2018. DLP. [Referred 14.02.2018]
https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

http://www.informit.com. 2017. Stateful firewalls. [Referred 28.10.2017]
http://www.informit.com/articles/article.aspx?p=373120

https://www.linux.fi. 2017. Software firewalls. [Referred 28.10.2017]
https://www.linux.fi/wiki/Iptables

https://technet.microsoft.com. 2017). Software firewalls. [Referred 28.10.2017]
https://technet.microsoft.com/en-us/library/dd364480(v=ws.10).aspx

https://www.paloaltonetworks.com. 2017. NextGen firewalls. [Referred 28.10.2017]
https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall

https://www.networkworld.com. 2017. NextGen firewalls. [Referred 28.10.2017]
https://www.networkworld.com/article/2161439/network-security/ssl-decryption-may-be-needed-for-security-reasons--but-employees-are-likely-to--fre.html

https://www.owasp.org. 2017. Web Application Firewall [Referred 28.10.2017]
https://www.owasp.org/index.php/Web_Application_Firewall

https://www.informationweek.com. 2017. Future of Firewalls. [Referred 5.12.2017]
https://www.informationweek.com/partner-perspectives/bitdefender/the-evolution-of-firewalls-past-present-and-future/a/d-id/1318814

http://searchsecurity.techtarget.com. 2017. IDS and IPS. [Referred 6.12.2017]
http://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPS-or-both

https://www.paloaltonetworks.com. 2017. [Referred 28.10.2017]
https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

https://www.sophos.com. 2017. Wireless security. [Referred 1.11.2017]
https://www.sophos.com/en-us/security-news-trends/best-practices/wi-fi.aspx

https://9to5mac.com. 2017. 2017. Wireless security. [Referred 1.11.2017]
https://9to5mac.com/2017/10/16/wifi-wpa2-hacked/

https://www.sans.org. 2017. Wireless security. [Referred 1.11.2017]
https://www.sans.org/reading-room/whitepapers/wireless/corporate-wireless-lan-risks-practices-mitigate-1350

https://msdn.microsoft.com. 2017. Centralized Account Management. [Referred 20.11.2017]
https://msdn.microsoft.com/en-us/library/bb727085.aspx

http://merabheja.com.2017. Centralized Account Management and Alternative Directory services. [Referred 20.11.2017]
http://merabheja.com/22-best-alternatives-to-microsoft-active-directory/

https://techterms.com. 2017. Active Directory. [Referred 20.11.2017]
https://techterms.com/definition/active_directory

https://technet.microsoft.com. 2017. Active Directory. [Referred 20.11.2017]
https://technet.microsoft.com/en-us/library/cc731204(v=ws.10).aspx

http://www.ciscozine.com. 2018. RADIUS. [Referred 16.01.2018]
http://www.ciscozine.com/access-network-devices-radius/

https://www.tutorialspoint.com. 2018. Diameter. [Referred 16.01.2018]
https://www.tutorialspoint.com/radius/what_is_diameter.htm

http://searchitchannel.techtarget.com. 2018. 802.1x. [Referred 17.01.2018]
http://searchmidmarketsecurity.techtarget.com/tip/Using-8021X-to-control-physical-access-to-LANs

http://searchitchannel.techtarget.com. 2018. 802.1x. [Referred 17.01.2018]
http://searchitchannel.techtarget.com/tip/Network-access-controlled-with-8021x

http://searchnetworking.techtarget.com. 2018. NIS and NIS+. [Referred 15.02.2018]
http://searchnetworking.techtarget.com/definition/NIS

https://docs.oracle.com. 2018. NIS and NIS+. [Referred 15.02.2018].
https://docs.oracle.com/cd/E19253-01/816-4558/abtrbl-20585/index.html

https://www.techopedia.com. 2018. [Referred 15.02.2018]
https://www.techopedia.com/definition/24149/network-monitoring

https://www.symantec.com. 2017. SIM, SEM and SIEM. [Referred 3.11.2017]
https://www.symantec.com/connect/articles/security-information-management-vs-security-event-management-vs-security-information-and-ev

https://www.techopedia.com. 2017. SIM, SEM and SIEM. [Referred 3.11.2017]
https://www.techopedia.com/7/31201/security/whats-the-difference-between-sem-sim-and-siem

https://scap.nist.gov. 2017. Security Scanning. [Referred 3.11.2017]
https://scap.nist.gov

https://www.sans.org. 2017. Security Scanning. [Referred 3.11.2017
https://www.sans.org/reading-room/whitepapers/threats/vulnerabilities-vulnerability-scanning-1195

https://nvd.nist.gov. 2017. CVSS scoring and security scanning. [Referred 3.11.2017]
https://nvd.nist.gov/vuln-metrics

https://blog.schneider-electric.com. 2017. Dual power-paths. [Referred 11.12.2017].
https://blog.schneider-electric.com/datacenter/2014/08/30/ensure-true-redundancy-dual-path-data-center-power-distribution-system/

http://www.datacenterjournal.com. 2017. Cooling systems. [Referred 15.11.2017].
http://www.datacenterjournal.com/basics-of-data-center-cooling/

https://avtech.com. 2017. Temperature and humidity. [Referred 15.09.2017].
https://avtech.com/articles/3647/recommended-data-center-temperature-humidity/

https://serverscheck.com. 2017. Temperature and humidity. [Referred 15.09.2017].
https://serverscheck.com/sensors/temperature_best_practices.asp

https://www.csoonline.com. 2017. Access control, surveillance, location. [Referred 15.11.2017]
https://www.csoonline.com/article/2112402/physical-security/physical-security-19-ways-to-build-physical-security-into-a-data-center.html

https://www.sans.org. 2017. Physical Security. [Referred 15.11.2017].
https://www.sans.org/reading-room/whitepapers/awareness/data-center-physical-security-checklist-416

https://www.itgovernance.co.uk. 2018. GDPR. [Referred 13.02.2018].
https://www.itgovernance.co.uk/dpa-and-gdpr-penalties
https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation

https://www.symantec.com. 2017. Energy Sector, Stuxnet. [Referred 11.12.2017]
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

https://www.wired.com. 2018. Energy Sector. Power grid hack. [Referred 21.01.2018]
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

https://www.hpe.com. Healthcare. 2018. [Referred 03.02.2018]
https://www.hpe.com/us/en/insights/articles/medical-IoT-devices-the-security-night-mare-that-keeps-cios-up-late-at-night-1709.html

https://www.theguardian.com. Ransomware healthcare. 2018. [Referred 21.01.2018]
https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack
https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransom-ware-nsa-uk-nhs

http://searchsecurity.techtarget.com. 2017. Data breaches, Advanced persistent threats, Denial of Service, ransomware. [Referred 6.11.2017]
http://searchsecurity.techtarget.com/definition/data-breach
http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT
http://searchsecurity.techtarget.com/definition/denial-of-service
http://searchsecurity.techtarget.com/definition/ransomware

https://www.sans.org. Healthcare. 2017. [Referred 11.12.2017]
https://www.sans.org/reading-room/whitepapers/analyst/threats-drive-improved-prac-tices-state-cybersecurity-health-care-organizations-35652

https://prajwaldesai.com. Peripherals. 2018. [Referred 24.01.2018]
https://prajwaldesai.com/how-to-disable-usb-devices-using-group-policy/

https://www.forbes.com. Healthcare. 2017. [Referred 11.12.2017]
https://www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction/#7f7a7f0021f8

https://www.wired.com. 2018. Machine learning/AI [Referred 17.02.2018]
https://www.wired.com/story/firewalls-dont-stop-hackers-ai-might/

https://www.eda.europa.eu. 2018. Machine learning/AI. [Referred 17.02.2018]
https://www.eda.europa.eu/webzine/issue14/cover-story/artificial-intelligence-(ai)-ena-bled-cyber-defence

http://www.directivecommunications.com. 2018. Biometric Authentication. [Referred 17.02.2018]
http://www.directivecommunications.com/do-passwords-have-a-place-in-the-future/

http://searchsecurity.techtarget.com. 2018. Biometric Authentication. [Referred 17.02.2018]
http://searchsecurity.techtarget.com/video/Say-hello-to-the-future-of-authentication-bye-to-passwords